(19)日本国特許庁（ＪＰ）　(12) **公表特許公報（Ａ）**　(11)特許出願公表番号
特表2003－536119
（P2003－536119A）
(43)公表日　平成15年12月２日(2003.12.2)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	５Ｂ０８５
15/00	３３０	15/00	３３０Ｚ	５Ｊ１０４
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６７５Ｂ	
9/32			６７５Ｄ	
			６０１Ｂ	

審査請求　未請求　　予備審査請求　有　　（全101頁）　　最終頁に続く

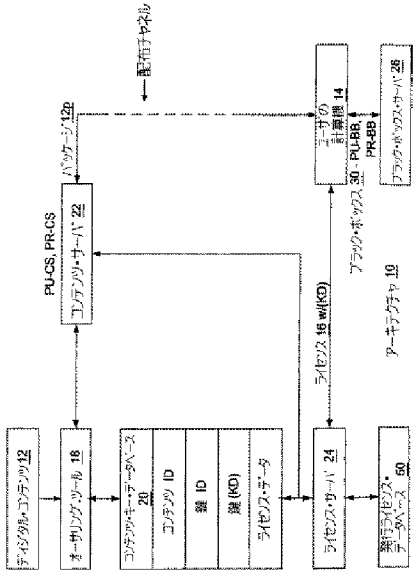
(21)出願番号　特願2000－608539(P2000－608539)
(86)（22)出願日　平成12年２月25日(2000.2.25)
(85)翻訳文提出日　平成13年９月27日(2001.9.27)
(86)国際出願番号　ＰＣＴ／ＵＳ００／０４９４７
(87)国際公開番号　ＷＯ００／０５９１５０
(87)国際公開日　平成12年10月５日(2000.10.5)
(31)優先権主張番号　６０／１２６，６１４
(32)優先日　平成11年３月27日(1999.3.27)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　０９／２９０，３６３
(32)優先日　平成11年４月12日(1999.4.12)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　マイクロソフト　コーポレイション
ＭＩＣＲＯＳＯＦＴ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国　ワシントン州　98052－6399　レッドモンド　ワン　マイクロソフト　ウェイ　（番地なし）
(72)発明者　ペイナド，マーカス
アメリカ合衆国ワシントン州98007，ベルビュー，ワンハンドレッドフォーティエイトス・アベニュー・ノースイースト　5007，ナンバー　イー207
(74)代理人　弁理士　社本　一夫　（外４名）

最終頁に続く

(54)【発明の名称】　デジタルデジタル権利管理の実施アーキテクチャおよび方法

(57)【要約】
デジタル権利を実施するための実施アーキテクチャおよび方法を開示する。コンテンツ・サーバからユーザの計算機にデジタル・コンテンツを配付し、ユーザの計算機は受信して、レンダリング・アプリケーションによってデジタル・コンテンツをレンダリングしようとする。レンダリング・アプリケーションは、デジタル権利管理（ＤＲＭ）システムを呼び出し、このようなＤＲＭシステムは、計算機に格納されておりデジタル・コンテンツに対応するいずれかのデジタル・ライセンスに基づいて、求められた態様でデジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう。権利が存在しない場合、このような権利を与え、デジタル・コンテンツに対応するデジタル・ライセンスを、ライセンス・サーバから要求し、ライセンス・サーバはデジタル・ライセンスをＤＲＭシステムに発行する。計算機は、発行されたデジタル・ライセンスを受信し、受信したデジタル・ライセンスを格納する。



【特許請求の範囲】

【請求項１】　デジタルデジタル権利管理実施アーキテクチャであって、該アーキテクチャが保護対象デジタルデジタル・コンテンツにおける権利を実施し、前記アーキテクチャが、

前記デジタルデジタル・コンテンツを配布するコンテンツ・サーバと、

前記デジタルデジタル・コンテンツに対応し、これとは別個の少なくとも１つのデジタルデジタル・ライセンスを発行するライセンス・サーバと、

前記配布したデジタルデジタル・コンテンツを受信し、当該デジタルデジタル・コンテンツに対応するあらゆるデジタルデジタル・ライセンスを受信しかつ格納する計算機と、

を備え、該計算機が、

前記デジタルデジタル・コンテンツをレンダリングするレンダリング・アプリケーションと、

前記レンダリング・アプリケーションが前記デジタルデジタル・コンテンツをレンダリングしようとするときに、当該レンダリング・アプリケーションが呼び出すデジタルデジタル権利管理（ＤＲＭ）システムであって、前記計算機に格納されており前記デジタルデジタル・コンテンツに対応するいずれかのデジタルデジタル・ライセンスに基づいて、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう、ＤＲＭシステムと、

を有する、デジタルデジタル権利実施アーキテクチャ。

【請求項２】　請求項１記載のアーキテクチャにおいて、前記コンテンツ・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記デジタルデジタル・コンテンツを配布する、アーキテクチャ。

【請求項３】　請求項２記載のアーキテクチャにおいて、前記コンテンツ・サーバはインターネットと結合して通信を行い、インターネットを通じて前記デジタルデジタル・コンテンツを配布する、アーキテクチャ。

【請求項４】　請求項１記載のアーキテクチャにおいて、前記ライセンス・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記少な

くとも１つのデジタルデジタル・ライセンスを発行する、アーキテクチャ。

【請求項５】　請求項４記載のアーキテクチャにおいて、前記ライセンス・サーバはインターネットと結合して通信を行い、インターネットを通じて前記少なくとも１つのデジタルデジタル・ライセンスを発行する、アーキテクチャ。

【請求項６】　請求項１記載のアーキテクチャにおいて、前記コンテンツ・サーバは携帯メディア・ライタと結合して通信を行い、該携帯メディア・ライタによって書き込んだ可搬媒体上で前記デジタルデジタル・コンテンツを配布し、前記可搬媒体を、光記憶媒体および磁気記憶媒体から成るグループから選択する、アーキテクチャ。

【請求項７】　請求項１記載のアーキテクチャにおいて、前記コンテンツ・サーバは暗号化形態で前記デジタルデジタル・コンテンツを配布する、アーキテクチャ。

【請求項８】　請求項７記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、

前記暗号化デジタルデジタル・コンテンツを解読する解読鍵と、

前記ライセンスによって与えられる権利の記述と、

を含み、前記暗号化デジタルデジタル・コンテンツは、前記ライセンス・サーバからこのようなライセンスを取得せずには、解読およびレンダリングが不可能である、アーキテクチャ。

【請求項９】　請求項８記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、更に、前記ライセンスを前記暗号化デジタルデジタル・コンテンツに結び付けるデジタルデジタル署名を含む、アーキテクチャ。

【請求項１０】　請求項１記載のアーキテクチャにおいて、前記ＤＲＭシステムが、前記計算機に格納されておりかつ前記デジタルデジタル・コンテンツに対応するいずれのデジタルデジタル・ライセンスに基づいても、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなＤＲＭシステムは、計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタルデジタル・コンテンツ

をレンダリングするデジタルデジタル・ライセンスを取得させる、アーキテクチャ。

【請求項１１】　請求項１記載のアーキテクチャにおいて、前記ＤＲＭシステムが、前記計算機に格納されておりかつ前記デジタルデジタル・コンテンツに対応するいずれのデジタルデジタル・ライセンスに基づいても、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなＤＲＭシステムは、計算機のユーザ側には何の行為を必要とせずに、前記ライセンス・サーバからデジタルデジタル・ライセンスを透過的に取得する、アーキテクチャ。

【請求項１２】　請求項１記載のアーキテクチャにおいて、前記ＤＲＭシステムは、デジタルデジタル・ライセンスを格納するライセンス・ストアを含む、アーキテクチャ。

【請求項１３】　請求項１記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスをこのようなデジタルデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項１４】　請求項１３記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスを、公開／秘密鍵技術によって、このようなデジタルデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項１５】　請求項１記載のアーキテクチャにおいて、前記ライセンス・サーバは、ＤＲＭシステムが前記ライセンスを順守することを当該ライセンス・サーバが信用する場合にのみ、このようなＤＲＭシステムにデジタルデジタル・ライセンスを発行する、アーキテクチャ。

【請求項１６】　請求項１５記載のアーキテクチャにおいて、前記コンテンツ・サーバは、前記デジタルデジタル・コンテンツを暗号化形態で配布し、前記ＤＲＭシステムは、このようなＤＲＭシステムのために解読および暗号化機能を実行する信頼ブラック・ボックスを含む、アーキテクチャ。

【請求項１７】　請求項１６記載のアーキテクチャにおいて、前記ブラック・ボックスは、前記解読および暗号化機能を実行するために、一意の公開／秘密

鍵対を含む、アーキテクチャ。

【請求項１８】　請求項１７記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタルデジタル・ライセンスを発行し、前記ライセンス要求がブラック・ボックス公開鍵を含み、前記ライセンス・サーバは、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタルデジタル・ライセンスの少なくとも一部を暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付ける、アーキテクチャ。

【請求項１９】　請求項１８記載のアーキテクチャにおいて、前記コンテンツ・サーバは前記デジタルデジタル・コンテンツを暗号化形態で配布し、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、前記暗号化デジタルデジタル・コンテンツを解読する解読鍵を含み、前記ライセンス・サーバは、前記ブラック・ボックス公開鍵にしたがって前記ライセンスにおける解読鍵を暗号化する、アーキテクチャ。

【請求項２０】　請求項１９記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、更に、前記ライセンスによって与えられる権利の記述を含み、前記暗号化デジタルデジタル・コンテンツは、前記ライセンス・サーバからこのようなライセンスを取得しなければ、解読しレンダリングすることが不可能であり、前記ライセンス・サーバは前記解読鍵にしたがって前記ライセンスにおける権利の記述を暗号化する、アーキテクチャ。

【請求項２１】　請求項１６記載のアーキテクチャにおいて、前記ブラック・ボックスはバージョン番号を含む、アーキテクチャ。

【請求項２２】　請求項２１記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタルデジタル・ライセンスを発行し、前記ライセンス要求が前記ブラック・ボックスのバージョン番号を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記ブラック・ボックスのバージョン番号が容認可能か否か判定を行い、前記ライセンス・サーバは、前記ブラック・ボックスのバージョン番号が容

認可能でないと判定したとき、前記ブラック・ボックスが更新されるまで、前記ライセンスの発行を拒絶し、前記アーキテクチャは、更に、更新ブラック・ボックスを前記ＤＲＭシステムに供給するブラック・ボックス・サーバを備える、アーキテクチャ。

【請求項２３】請求項１６記載のアーキテクチャにおいて、前記ブラック・ボックスは、承認された証明機関が供給する証明機関署名を含む、アーキテクチャ。

【請求項２４】　請求項２３記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタルデジタル・ライセンスを発行し、前記ライセンス要求が前記証明機関署名を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記証明機関署名が有効か否か判定を行なう、アーキテクチャ。

【請求項２５】　請求項１５記載のアーキテクチャにおいて、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンスは、前記ライセンスによって与えられる権利の記述を含み、前記ＤＲＭシステムは、前記権利の記述を評価し、レンダリング・アプリケーションによるデジタルデジタル・コンテンツのレンダリングが前記ライセンスの権利の記述に応じたものである場合、このようなレンダリグを許可する、信頼ライセンス評価部を含む、アーキテクチャ。

【請求項２６】　請求項１記載のアーキテクチャであって、更に、前記ライセンス・サーバが発行するデジタルデジタル・ライセンスに関する情報を維持する発行ライセンス・データベースを備え、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベースにおける情報に基づいて、その再発行を可能とした、アーキテクチャ。

【請求項２７】　請求項１記載のアーキテクチャであって、更に、前記コンテンツ・サーバが配布する前記デジタルデジタル・コンテンツを、当該アーキテクチャに適した形態でオーサリングするオーサリング・ツールを備える、アーキテクチャ。

【請求項２８】　請求項２７記載のアーキテクチャにおいて、前記オーサリ

ング・ツールは、解読鍵にしたがって前記デジタルデジタル・コンテンツを暗号化し、前記デジタルデジタル・コンテンツおよび前記暗号化鍵に関する情報をコンテンツ鍵データベースに格納する、アーキテクチャ。

【請求項２９】　請求項２８記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記デジタルデジタル・コンテンツに対応するライセンスの発行に先立って、前記コンテンツ鍵データベース内にある前記デジタルデジタル・コンテンツおよび前記暗号化鍵に関する情報にアクセスし、このようなライセンスの発行に伴う前記解読鍵を含む、アーキテクチャ。

【請求項３０】　デジタルデジタル権利管理の実施方法であって、該方法が保護対象デジタルデジタル・コンテンツにおける権利実施を行い、

コンテンツ・サーバからユーザの計算機に前記デジタルデジタル・コンテンツを配布するステップと、

前記計算機において前記配布されたデジタルデジタル・コンテンツを受信するステップと、

レンダリング・アプリケーションが前記デジタルデジタル・コンテンツのレンダリングを行なおうとするステップと、

このようなレンダリング・アプリケーションが前記デジタルデジタル・コンテンツをレンダリングしようとする際に、前記レンダリング・アプリケーションがデジタルデジタル権利管理（ＤＲＭ）システムを呼び出すステップと、

前記計算機に格納されており前記デジタルデジタル・コンテンツに対応するいずれかのデジタルデジタル・ライセンスに基づいて、前記ＤＲＭシステムが、求められた態様で前記デジタルデジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なうステップと、

前記権利が存在する場合、

このような権利を与え、かつ前記デジタルデジタル・コンテンツに対応しこれとは別個デジタルデジタル・ライセンスを、ライセンス・サーバから要求するステップと、

前記ライセンス・サーバが、前記ＤＲＭシステムに前記デジタルデジタル・ライセンスを発行するステップと、

前記計算機が、前記ライセンス・サーバからの前記デジタルデジタル・コンテンツに対応する、前記発行されたデジタルデジタル・ライセンスを受信するステップと、

前記受信したデジタルデジタル・ライセンスを前記計算機上に格納するステップと、

から成る方法。

【請求項３１】　請求項３０記載の方法において、前記配布するステップは、ネットワークを通じて前記デジタルデジタル・コンテンツを配布するステップから成る、方法。

【請求項３２】　請求項３１記載の方法において、前記配布するステップは、インターネットを通じて前記デジタルデジタル・コンテンツを配布するステップから成る、方法。

【請求項３３】　請求項３０記載の方法において、前記発行するステップは、ネットワークを通じて前記デジタルデジタル・ライセンスを発行するステップから成る、方法。

【請求項３４】　請求項３３記載の方法において、前記発行するステップは、インターネットを通じて前記デジタルデジタル・ライセンスを発行するステップから成る、方法。

【請求項３５】　請求項３０記載の方法において、前記配布するステップは、光記憶媒体および磁気記憶媒体から成るグループから選択した可搬媒体上で前記デジタルデジタル・コンテンツを配布するステップから成る、方法。

【請求項３６】　請求項３０記載の方法において、前記配布するステップは、前記デジタルデジタル・コンテンツを暗号化形態で配布するステップから成る、方法。

【請求項３７】　請求項３６記載の方法であって、更に、前記デジタルデジタル・コンテンツに対応する各デジタルデジタル・ライセンス毎に、

前記暗号化デジタルデジタル・コンテンツを解読する解読鍵と、

前記ライセンスによって与えられる権利の記述とを含ませるステップを含み、

前記ライセンス・サーバからこのようなライセンスを取得しなければ、前記暗

号化デジタル・コンテンツを解読しレンダリングすることを不可能とした、方法。

【請求項３８】　請求項３７記載の方法において、前記含ませるステップは、前記デジタル・コンテンツに対応する各ライセンス毎に、前記ライセンスを前記暗号化デジタル・コンテンツに結び付けるデジタル署名を含ませるステップから成る、方法。

【請求項３９】　請求項３０記載の方法において、前記デジタル・ライセンスを要求するステップは、前記ＤＲＭシステムが計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタル・コンテンツをレンダリングするデジタル・ライセンスを取得するステップから成る、方法。

【請求項４０】　請求項３０記載の方法において、前記デジタル・ライセンスを要求するステップは、計算機ユーザの側では何の行為も必要とせずに、前記ＤＲＭシステムが、前記ライセンス・サーバからデジタル・ライセンスを透過的に取得するステップから成る、方法。

【請求項４１】　請求項３０記載の方法において、前記格納するステップは、前記ＤＲＭシステムが、受信した前記ライセンス・サーバを前記ＤＲＭシステムのライセンス・ストアに格納するステップから成る、方法。

【請求項４２】　請求項３０記載の方法であって、更に、前記ライセンス・サーバが、前記デジタル・ライセンスを前記対応するデジタル・コンテンツに結び付けるステップを含む、方法。

【請求項４３】　請求項４２記載の方法であって、公開／秘密鍵技術によって、前記ライセンス・サーバが前記デジタル・ライセンスを前記対応するデジタル・コンテンツに結び付けるステップを含む、方法。

【請求項４４】　請求項３０記載の方法において、前記発行するステップは、前記ＤＲＭシステムが前記ライセンスを順守することを、前記ライセンス・サーバが信用する場合にのみ、前記ライセンス・サーバが前記デジタル・ライセンスをこのようなＤＲＭシステムに発行するステップから成る、方法。

【請求項４５】　請求項４４記載の方法において、前記配布するステップは、前記コンテンツ・サーバが前記デジタル・コンテンツを暗号化形態で配布する

ステップから成り、更に、前記ＤＲＭシステムにおいて信頼ブラック・ボックスを用いて、このようなＤＲＭシステムのために解読および暗号化機能を実行するステップを含む、方法。

【請求項４６】　請求項４５記載の方法において、前記ブラック・ボックスは公開／秘密鍵対を含み、前記デジタル・ライセンスを要求するステップは、前記要求にブラック・ボックス公開鍵を含ませるステップから成り、更に、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタル・ライセンスの少なくとも一部を前記ライセンス・サーバが暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付けるステップを含む、方法。

【請求項４７】　請求項４６記載の方法において、前記配布するステップは、前記デジタル・コンテンツを暗号化形態で配布するステップから成り、更に、

前記デジタル・コンテンツに対応する各デジタル・ライセンス毎に、前記暗号化デジタル・コンテンツを解読する解読鍵を含ませるステップと、

前記ブラック・ボックス公開鍵にしたがって、前記ライセンス・サーバが前記ライセンス内にある前記解読鍵を暗号化するステップと、

を含む、方法。

【請求項４８】　請求項４７記載の方法であって、更に、

前記デジタル・コンテンツに対応する各デジタル・ライセンス毎に、前記ライセンスによって与えられる権利の記述を含ませるステップであって、前記ライセンス・サーバからのこのようなライセンスを取得しなければ、前記暗号化デジタル・コンテンツを解読しレンダリングすることを不可能とする、ステップと、

前記解読鍵にしたがって前記ライセンス・サーバが前記ライセンス内の権利の記述を暗号化するステップと、

を含む、方法。

【請求項４９】　請求項４５記載の方法において、前記ブラック・ボックスはバージョン番号を含み、前記デジタル・ライセンスを要求するステップは、前記ブラック・ボックスのバージョン番号を前記要求内に含ませるステップから成り、更に、

前記ライセンスの発行に先立って、前記ライセンス・サーバが前記ブラック・ボックスのバージョン番号が容認可能か否か判定を行なうステップと、

前記ブラック・ボックスのバージョン番号が容認可能でないと判定したとき、前記ライセンス・サーバが、前記ブラック・ボックスを更新するまで、前記ライセンスの発行を拒絶するステップと、

を含み、前記アーキテクチャが、前記ＤＲＭシステムに更新ブラック・ボックスを供給するブラック・ボックス・サーバを備える、方法。

【請求項５０】　請求項４５記載の方法において、前記ブラック・ボックスは、承認された証明機関が供給する証明機関署名を含み、前記デジタル・ライセンスを要求するステップは、前記証明機関署名を含ませ、前記ライセンスの発行に先立って、前記ライセンス・サーバが前記証明機関署名が有効か否か判定を行なうステップを含む、方法。

【請求項５１】　請求項４４記載の方法において、前記デジタル・ライセンスを発行するステップは、前記ライセンスによって与えられる権利の記述を前記デジタル・ライセンスに含ませるステップを含み、更に、

前記ＤＲＭシステムの信頼ライセンス評価部が、前記権利の記述を評価するステップと、

前記レンダリング・アプリケーションによる前記デジタル・コンテンツのレンダリングが、前記ライセンスの権利の記述に応じたものである場合にのみ、このようなレンダリングを許可するステップと、

を含む、方法。

【請求項５２】　請求項３０記載の方法であって、更に、前記ライセンス・サーバが発行するデジタル・ライセンスに関する情報を発行ライセンス・データベースに維持するステップを含み、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベース内にある情報に基づいて、その再発行を可能とする、方法。

【請求項５３】　請求項３０記載の方法であって、更に、オーサリング・ツールによって、前記コンテンツ・サーバが配布したデジタル・コンテンツを、前記アーキテクチャに適した形態でオーサリングするステップを含む、方法。

【請求項５４】　請求項５３記載の方法において、前記オーサリングするステップは、

解読鍵にしたがって前記デジタル・コンテンツを暗号化するステップと、

前記デジタル・コンテンツおよび前記暗号化鍵に関する情報を、コンテンツ鍵データベースに格納するステップと、

を含む、方法。

【請求項５５】　請求項５４記載の方法において、前記デジタル・ライセンスを発行するステップは、

前記デジタル・コンテンツに対応するライセンスの発行に先立って、前記ライセンス・サーバが前記コンテンツ鍵データベース内の前記デジタル・コンテンツおよび前記暗号化鍵に関する情報にアクセスするステップと、

このような発行されたライセンスに、前記解読鍵を含ませるステップと、

を含む、方法。

【請求項５６】　デジタル権利管理実施アーキテクチャであって、該アーキテクチャは保護対象デジタル・コンテンツにおける権利を実施し、

ネットワークと通信するように結合され、前記デジタル・コンテンツを前記ネットワークを通じて配布するコンテンツ・サーバと、

前記デジタル・コンテンツに対応しこれとは別個の少なくとも１つのデジタル・ライセンスを発行するライセンス・サーバであって、前記ネットワークと通信するように結合され、前記少なくとも１つのデジタル・ライセンスを前記ネットワークを通じて発行する、ライセンス・サーバと、

前記ネットワークと通信するように結合され、前記配布されたデジタル・コンテンツを受信し、かつ前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスを受信する計算機と、

から成り、前記計算機が、

前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスを格納するメモリと、

前記デジタル・コンテンツをレンダリングしようとするレンダリング・アプリケーションと、

前記レンダリング・アプリケーションが前記デジタル・コンテンツをレンダリングしようとするときに、当該レンダリング・アプリケーションが呼び出すデジタル権利管理（ＤＲＭ）システムであって、前記計算機に格納されており前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスに基づいて、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう、ＤＲＭシステムと、
を有する、デジタル権利実施アーキテクチャ。

【請求項５７】　請求項５６記載のアーキテクチャにおいて、前記コンテンツ・サーバはインターネットと結合して通信を行い、インターネットを通じて前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項５８】　請求項５６記載のアーキテクチャにおいて、前記ライセンス・サーバはインターネットと結合して通信を行い、インターネットを通じて前記少なくとも１つのデジタル・ライセンスを発行する、アーキテクチャ。

【請求項５９】　請求項５６記載のアーキテクチャにおいて、前記コンテンツ・サーバは携帯メディア・ライタと結合して通信を行い、該携帯メディア・ライタによって書き込んだ可搬媒体上で前記デジタル・コンテンツを配布し、前記可搬媒体を、光記憶媒体および磁気記憶媒体から成るグループから選択し、前記計算機は、前記可搬媒体に対応し、該可搬媒体を受け入れ読み取りを行なう可搬媒体リーダを含む、アーキテクチャ。

【請求項６０】　請求項５６記載のアーキテクチャにおいて、前記コンテンツ・サーバは暗号化形態で前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項６１】　請求項６０記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、
前記暗号化デジタル・コンテンツを解読する解読鍵と、
前記ライセンスによって与えられる権利の記述と、
を含み、前記ライセンス・サーバからこのようなライセンスを取得せずには、前記暗号化デジタル・コンテンツを解読しレンダリングすることを不可能とした、アーキテクチャ。

【請求項６２】　請求項６１記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスを前記暗号化デジタル・コンテンツに結び付けるデジタル署名を含む、アーキテクチャ。

【請求項６３】　請求項５６記載のアーキテクチャにおいて、前記ＤＲＭシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなＤＲＭシステムは、計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタル・コンテンツをレンダリングするデジタル・ライセンスを取得させる、アーキテクチャ。

【請求項６４】　請求項５６記載のアーキテクチャにおいて、前記ＤＲＭシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、このようなＤＲＭシステムは、計算機のユーザ側には何の行為を必要とせずに、前記ライセンス・サーバからデジタル・ライセンスを透過的に取得する、アーキテクチャ。

【請求項６５】　請求項５６記載のアーキテクチャにおいて、前記ＤＲＭシステムは、デジタル・ライセンスを格納するライセンス・ストアを含む、アーキテクチャ。

【請求項６６】　請求項５６記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスをこのようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項６７】　請求項６６記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスを、公開／秘密鍵技術によって、このようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項６８】　請求項５６記載のアーキテクチャにおいて、前記ライセンス・サーバは、ＤＲＭシステムが前記ライセンスを順守することを当該ライセンス・サーバが信用する場合にのみ、このようなＤＲＭシステムにデジタル・ライ

センスを発行する、アーキテクチャ。

【請求項６９】　請求項６８記載のアーキテクチャにおいて、前記コンテンツ・サーバは、前記デジタル・コンテンツを暗号化形態で配布し、前記ＤＲＭシステムは、このようなＤＲＭシステムのために解読および暗号化機能を実行する信頼ブラック・ボックスを含む、アーキテクチャ。

【請求項７０】　請求項６９記載のアーキテクチャにおいて、前記ブラック・ボックスは、前記解読および暗号化機能を実行するために、一意の公開／秘密鍵対を含む、アーキテクチャ。

【請求項７１】　請求項７０記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求がブラック・ボックス公開鍵を含み、前記ライセンス・サーバは、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタル・ライセンスの少なくとも一部を暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付ける、アーキテクチャ。

【請求項７２】　請求項７１記載のアーキテクチャにおいて、前記コンテンツ・サーバは前記デジタル・コンテンツを暗号化形態で配布し、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記暗号化デジタル・コンテンツを解読する解読鍵を含み、前記ライセンス・サーバは、前記ブラック・ボックス公開鍵にしたがって前記ライセンスにおける解読鍵を暗号化する、アーキテクチャ。

【請求項７３】　請求項７２記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスによって与えられる権利の記述を含み、前記ライセンス・サーバからこのようなライセンスを取得しなければ、前記暗号化デジタル・コンテンツを解読しレンダリングすることが不可能であり、前記ライセンス・サーバは前記解読鍵にしたがって前記ライセンスにおける権利の記述を暗号化する、アーキテクチャ。

【請求項７４】　請求項６９記載のアーキテクチャにおいて、前記ブラック・ボックスはバージョン番号を含む、アーキテクチャ。

【請求項７５】　請求項７４記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記ブラック・ボックスのバージョン番号を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記ブラック・ボックスのバージョン番号が容認可能か否か判定を行い、前記ライセンス・サーバは、前記ブラック・ボックスのバージョン番号が容認可能でないと判定したとき、前記ブラック・ボックスが更新されるまで、前記ライセンスの発行を拒絶し、前記アーキテクチャは、更に、更新ブラック・ボックスを前記ＤＲＭシステムに供給するブラック・ボックス・サーバを備える、アーキテクチャ。

【請求項７６】請求項６９記載のアーキテクチャにおいて、前記ブラック・ボックスは、承認された証明機関によって供給される証明機関署名を含む、アーキテクチャ。

【請求項７７】　請求項７６記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記証明機関署名を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記証明機関署名が有効か否か判定を行なう、アーキテクチャ。

【請求項７８】　請求項６８記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記ライセンスによって与えられる権利の記述を含み、前記ＤＲＭシステムは、前記権利の記述を評価し、レンダリング・アプリケーションによるデジタル・コンテンツのレンダリングが前記ライセンスの権利の記述に応じたものである場合、このようなレンダリグを許可する、信頼ライセンス評価部を含む、アーキテクチャ。

【請求項７９】　請求項５６記載のアーキテクチャであって、更に、前記ライセンス・サーバが発行するデジタル・ライセンスに関する情報を維持する発行ライセンス・データベースを備え、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベースにおける情報に基づいて、その再発行を可能とした、アーキテクチャ。

【請求項８０】　請求項５６記載のアーキテクチャであって、更に、前記コンテンツ・サーバが配布する前記デジタル・コンテンツを、当該アーキテクチャに適した形態でオーサリングするオーサリング・ツールを備える、アーキテクチャ。

【請求項８１】　請求項８０記載のアーキテクチャにおいて、前記オーサリング・ツールは、解読鍵にしたがって前記デジタル・コンテンツを暗号化し、前記デジタル・コンテンツおよび前記暗号化鍵に関する情報をコンテンツ鍵データベースに格納する、アーキテクチャ。

【請求項８２】　請求項８１記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記デジタル・コンテンツに対応するライセンスの発行に先立って、前記コンテンツ鍵データベース内にある前記デジタル・コンテンツおよび前記暗号化鍵に関する情報にアクセスし、このようなライセンスの発行に伴う前記解読鍵を含む、アーキテクチャ。

【請求項８３】　デジタル権利管理実施アーキテクチャであって、該アーキテクチャは保護対象デジタル・コンテンツにおける権利を実施し、前記アーキテクチャが、

前記アーキテクチャに適した形態で前記デジタル・コンテンツのオーサリングを行なうオーサリング・ツールと、

前記オーサリング・ツールから前記デジタル・コンテンツを受け取り、該デジタル・コンテンツを配布するコンテンツ・サーバと、

前記デジタル・コンテンツに対応し、これとは別個の少なくとも１つのデジタル・ライセンスを発行するライセンス・サーバであって、計算機が、前記配布したデジタル・コンテンツを受信し、当該デジタル・コンテンツに対応するあらゆるデジタル・ライセンスを受信しかつ格納する、ライセンス・サーバと、

を備え、該計算機が、

前記デジタル・コンテンツをレンダリングするレンダリング・アプリケーションと、

前記レンダリング・アプリケーションが前記デジタル・コンテンツをレンダリングしようとするときに、当該レンダリング・アプリケーションが呼び出すデジ

タル権利管理（ＤＲＭ）システムであって、前記計算機に格納されており前記デジタル・コンテンツに対応するいずれかのデジタル・ライセンスに基づいて、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在するか否か判定を行なう、ＤＲＭシステムと、
を有する、デジタル権利実施アーキテクチャ。

【請求項８４】　請求項８３記載のアーキテクチャにおいて、前記コンテンツ・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項８５】　請求項８４記載のアーキテクチャにおいて、前記コンテンツ・サーバはインターネットと結合して通信を行い、インターネットを通じて前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項８６】　請求項８３記載のアーキテクチャにおいて、前記ライセンス・サーバはネットワークと結合して通信を行い、該ネットワークを通じて前記少なくとも１つのデジタル・ライセンスを発行する、アーキテクチャ。

【請求項８７】　請求項８６記載のアーキテクチャにおいて、前記ライセンス・サーバはインターネットと結合して通信を行い、インターネットを通じて前記少なくとも１つのデジタル・ライセンスを発行する、アーキテクチャ。

【請求項８８】　請求項８３記載のアーキテクチャにおいて、前記コンテンツ・サーバは携帯メディア・ライタと結合して通信を行い、該携帯メディア・ライタによって書き込んだ可搬媒体上で前記デジタル・コンテンツを配布し、前記可搬媒体を、光記憶媒体および磁気記憶媒体から成るグループから選択する、アーキテクチャ。

【請求項８９】　請求項１記載のアーキテクチャにおいて、前記コンテンツ・サーバは暗号化形態で前記デジタル・コンテンツを配布する、アーキテクチャ。

【請求項９０】　請求項８９記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、
前記暗号化デジタル・コンテンツを解読する解読鍵と、
前記ライセンスによって与えられる権利の記述と、

を含み、前記ライセンス・サーバからこのようなライセンスを取得せずには、前記暗号化デジタル・コンテンツを解読しレンダリングすることを不可能とした、アーキテクチャ。

【請求項９１】　請求項９０記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスを前記暗号化デジタル・コンテンツに結び付けるデジタル署名を含む、アーキテクチャ。

【請求項９２】　請求項８３記載のアーキテクチャにおいて、前記ＤＲＭシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、計算機のユーザを前記ライセンス・サーバに差し向け、求められた態様でこのようなデジタル・コンテンツをレンダリングするデジタル・ライセンスを取得させる、アーキテクチャ。

【請求項９３】　請求項８３記載のアーキテクチャにおいて、前記ＤＲＭシステムが、前記計算機に格納されておりかつ前記デジタル・コンテンツに対応するいずれのデジタル・ライセンスに基づいても、求められた態様で前記デジタル・コンテンツをレンダリングする権利が存在しないと判定した場合、前記ＤＲＭシステムは、計算機のユーザ側には何の行為を必要とせずに、前記ライセンス・サーバからデジタル・ライセンスを透過的に取得する、アーキテクチャ。

【請求項９４】　請求項８３記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスをこのようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項９５】　請求項９４記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスを、公開／秘密鍵技術によって、このようなデジタル・コンテンツに結び付けてある、アーキテクチャ。

【請求項９６】　請求項８３記載のアーキテクチャにおいて、前記ライセンス・サーバは、ＤＲＭシステムが前記ライセンスを順守することを当該ライセンス・サーバが信用する場合にのみ、このようなＤＲＭシステムにデジタル・ライ

センスを発行する、アーキテクチャ。

【請求項９７】　請求項９６記載のアーキテクチャにおいて、前記コンテンツ・サーバは、前記デジタル・コンテンツを暗号化形態で配布し、前記ＤＲＭシステムは、このようなＤＲＭシステムのために解読および暗号化機能を実行する信頼ブラック・ボックスを含み、前記ブラック・ボックスは、前記解読および暗号化機能を実行するために、一意の公開／秘密鍵対を含み、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求がブラック・ボックス公開鍵を含み、前記ライセンス・サーバは、このようなライセンスの発行に先立って、前記ブラック・ボックス公開鍵にしたがって前記デジタル・ライセンスの少なくとも一部を暗号化することにより、このようなライセンスをこのようなブラック・ボックスに結び付ける、アーキテクチャ。

【請求項９８】　請求項９７記載のアーキテクチャにおいて、前記コンテンツ・サーバは前記デジタル・コンテンツを暗号化形態で配布し、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記暗号化デジタル・コンテンツを解読する解読鍵を含み、前記ライセンス・サーバは、前記ブラック・ボックス公開鍵にしたがって前記ライセンスにおける解読鍵を暗号化する、アーキテクチャ。

【請求項９９】　請求項９８記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、更に、前記ライセンスによって与えられる権利の記述を含み、前記ライセンス・サーバからこのようなライセンスを取得しなければ、前記暗号化デジタル・コンテンツを解読しレンダリングすることが不可能であり、前記ライセンス・サーバは前記解読鍵にしたがって前記ライセンスにおける権利の記述を暗号化する、アーキテクチャ。

【請求項１００】　請求項９７記載のアーキテクチャにおいて、前記ブラック・ボックスはバージョン番号を含み、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記ブラック・ボックスのバージョン番号を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記ブラック・ボックス

のバージョン番号が容認可能か否か判定を行い、前記ライセンス・サーバは、前記ブラック・ボックスのバージョン番号が容認可能でないと判定したとき、前記ブラック・ボックスが更新されるまで、前記ライセンスの発行を拒絶し、前記アーキテクチャは、更に、更新ブラック・ボックスを前記ＤＲＭシステムに供給するブラック・ボックス・サーバを備える、アーキテクチャ。

【請求項１０１】　請求項９７記載のアーキテクチャにおいて、前記ブラック・ボックスは、承認された証明機関によって供給される証明機関署名を含み、前記ライセンス・サーバは、前記ＤＲＭシステムからのライセンス要求に応答して各デジタル・ライセンスを発行し、前記ライセンス要求が前記証明機関署名を含み、前記ライセンス・サーバは、前記ライセンスの発行に先立って、前記証明機関署名が有効か否か判定を行なう、アーキテクチャ。

【請求項１０２】　請求項９６記載のアーキテクチャにおいて、前記デジタル・コンテンツに対応する各デジタル・ライセンスは、前記ライセンスによって与えられる権利の記述を含み、前記ＤＲＭシステムは、前記権利の記述を評価し、レンダリング・アプリケーションによるデジタル・コンテンツのレンダリングが前記ライセンスの権利の記述に応じたものである場合、このようなレンダリグを許可する、信頼ライセンス評価部を含む、アーキテクチャ。

【請求項１０３】　請求項８３記載のアーキテクチャであって、更に、前記ライセンス・サーバが発行するデジタル・ライセンスに関する情報を維持する発行ライセンス・データベースを備え、前記計算機が受信したライセンスを紛失した場合、前記発行ライセンス・データベースにおける情報に基づいて、その再発行を可能とした、アーキテクチャ。

【請求項１０４】　請求項８３記載のアーキテクチャにおいて、前記オーサリング・ツールは、解読鍵にしたがって前記デジタル・コンテンツを暗号化し、前記デジタル・コンテンツおよび前記暗号化鍵に関する情報をコンテンツ鍵データベースに格納する、アーキテクチャ。

【請求項１０５】　請求項１０４記載のアーキテクチャにおいて、前記ライセンス・サーバは、前記デジタル・コンテンツに対応するライセンスの発行に先立って、前記コンテンツ鍵データベース内にある前記デジタル・コンテンツおよ

び前記暗号化鍵に関する情報にアクセスし、このようなライセンスの発行に伴う前記解読鍵を含む、アーキテクチャ。

【発明の詳細な説明】

【０００１】

（関連出願に対する引用）

本願は、”ENFORCEMENT ARCHITECHTURE AND METHOD FOR DIGITAL RIGHTS MANAGEMENT”（デジタル権利管理実施アーキテクチャおよび方法）と題し、弁理士整理番号MSFT-0063の下で１９９９年３月２７日に出願した米国仮出願第60/126,614号の優先権を主張する。

【０００２】

（発明の分野）

本発明は、デジタル・コンテンツにおける権利実施アーキテクチャに関する。更に特定すれば、本発明は、デジタル・コンテンツのユーザが取得した実施権（licence right）によって指定されるパラメータのみに応じて暗号化デジタル・コンテンツに対するアクセスを許可するようにした、実施アーキテクチャに関する。

【０００３】

（発明の背景）

デジタル権利の管理および実施は、デジタル・オーディオ、デジタル・ビデオ、デジタル・テキスト、デジタル・データ、デジタル・マルチメディア等のようなデジタル・コンテンツに関して、このようなデジタル・コンテンツをユーザに配付する場合に非常に望ましい。典型的な配付方式は、磁気（フロッピ）ディスク、磁気テープ、光（コンパクト）ディスク（ＣＤ）等のような有形デバイスや、電子掲示板、電子ネットワーク、インターネット等のような無形媒体を含む。ユーザが受信すると、ユーザはメディア・プレーヤ、パーソナル・コンピュータのような適当なレンダリング・デバイスの助けによって、デジタル・コンテンツのレンダリング（rendering）即ち「再生」を行なう。

【０００４】

典型的に、コンテンツ所有者即ち著作者、出版社、放送会社等（以下「コンテンツ所有者」）のような権利保有者は、このようなデジタル・コンテンツをライセンス料またはその他の何らかの対価との交換によってユーザ即ち受取人に販売

したい。このようなコンテンツ所有者は、選択が認められれば、ユーザがこのように販売したデジタル・コンテンツを用いて行なえることを制限したいことも多いであろう。例えば、コンテンツ所有者は、ユーザがこのようなコンテンツをコピーしたり、第２のユーザに再配付することを、少なくともこのような第２のユーザがコンテンツ所有者にライセンス料を拒否するような態様では、制約したいであろう。

【０００５】

加えて、コンテンツ所有者は、異なるライセンス料で異なる種類の使用許諾を購入する柔軟性をユーザに提供しつつ、同時に実際にいかなるライセンスの種類を購入しようがユーザにその条件を維持させたいこともある。例えば、コンテンツ所有者は、販売したデジタル・コンテンツの再生を限定回数のみ、ある合計時間だけ、ある種の機械においてのみ、ある種のメディア・プレーヤにおいてのみ、ある種のユーザにのみ再生することを許可したい場合もある。

【０００６】

しかしながら、販売を行なった後、このようなコンテンツ所有者は、デジタル・コンテンツの管理を行なうにしても、極僅かである。これは、特に、実際にあらゆる新製品または最新のパーソナル・コンピュータが、このようなデジタル・コンテンツの正確なデジタル・コピーを作成するため、ならびにこのような正確なデジタル・コピーを書き込み可能な磁気または光ディスクにダウンロードするため、またはこのような正確なコピーをあらゆる宛先にインターネットのようなネットワークを通じて送るために必要なソフトウエアおよびハードウエアを含んでいるという事実を考慮すると、問題である。

【０００７】

勿論、ライセンス料が得られた場合法的処置の一部として、コンテンツ所有者はデジタル・コンテンツのユーザに、このようなデジタル・コンテンツの再配付をしないことを約束するように求めることはできる。しかしながら、このような約束は容易に行われ、容易に破られる。コンテンツ所有者は、大抵の場合暗号化および解読を伴う、いくつかの公知のセキュリティ・デバイスのいずれかによってこのような再配付を防止しようとすることもできる。しかしながら、決意の弱

いユーザ（mildly determined user）に、暗号化デジタル・コンテンツを解読し、このようなデジタル・コンテンツを無暗号化形態で保存し、次いでこれを再配付する、ということを禁止できない場合が多い。

【０００８】

したがって、デジタル・コンテンツの任意の形態のレンダリング即ち再生を管理可能にする実施アーキテクチャおよび方法を提供する必要性がある。この場合、管理は柔軟性があり、このようなデジタル・コンテンツのコンテンツ所有者によって定義可能とする。また、パーソナル・コンピュータのような計算機上においてレンダリング環境を管理する必要性もある。この場合、レンダリング環境は、このような実施アーキテクチャの少なくとも一部を含む。このようなレンダリング環境の管理によって、デジタル・コンテンツはコンテンツ所有者の制御下にはない計算機上でレンダリングされるものの、コンテンツ所有者が指定するようにのみデジタル・コンテンツをレンダリングすることが可能になる。

【０００９】

更に、計算機上において信頼コンポーネント（trusted component）を走らせ、このような計算機のユーザがコンテンツ所有者が許可しない方法でこのようなデジタル・コンテンツにアクセスしようとしても、信頼コンポーネントがコンテンツ所有者の権利を、１片のデジタル・コンテンツに関してこのような計算機上で実施することも必要とされている。単なる一例として、このような信頼ソフトウエア・コンポーネントは、計算機のユーザが、コンテンツ所有者が許可する場合を除いて、このようなデジタル・コンテンツのコピーを作成することを防止する。

（発明の概要）

前述の必要性は、少なくとも部分的にデジタル権利管理実施アーキテクチャおよび方法によって満たされる。このアーキテクチャおよび方法は、インターネット、光ディスク等において利用可能な保護（保証）デジタル・コンテンツにおいて権利を実施する。コンテンツを利用可能にするために、アーキテクチャは、コンテンツ・サーバを含み、ここからインターネット等を通じて暗号化した形態でデジタル・コンテンツにアクセス可能である。コンテンツ・サーバは、暗号化デ

ジタル・コンテンツを供給し、光ディスク等に記録することも可能であり、暗号化デジタル・コンテンツは光ディスク自体で配付することもできる。コンテンツ・サーバでは、デジタル・コンテンツを暗号化鍵を用いて暗号化し、公開／秘密鍵技術を用いて、ユーザの計算機またはクライアント・マシン上でデジタル・コンテンツをデジタル・ライセンスと結び付ける。

【００１０】

ユーザがデジタル・コンテンツを計算機上でレンダリングしようとすると、レンダリング・アプリケーションが、このようなユーザの計算機上でデジタル権利管理（ＤＲＭ）システムを呼び出す。ユーザが最初にデジタル・コンテンツをレンダリングしようとしている場合、ＤＲＭシステムはユーザをライセンス・サーバに差し向け、このようなデジタル・コンテンツをレンダリングするライセンスを、求められた態様で取得させるか、あるいはユーザ側では何の行為も必要とせずに、このようなライセンス・サーバからこのようなライセンスを透過的に取得する。ライセンスは以下を含む。

【００１１】

－暗号化デジタル・コンテンツを解読する解読鍵（ＫＤ）

－ライセンスおよび関連条件（開始日、終了日、再生回数等）によって与えられる権利（再生、コピー等）の記述。このような記述はデジタル的に読み取り可能な形態である。

【００１２】

－ライセンスの保全を確保するデジタル署名

ユーザは、このようなライセンスをライセンス・サーバから取得しなければ、暗号化デジタル・コンテンツの解読やレンダリングを行なうことができない。取得したライセンスは、ユーザの計算機においてライセンス・ストアに格納される。

【００１３】

重要なことは、ライセンス・サーバは「信頼」された（即ち、それ自体で認証可能な）ＤＲＭシステムにライセンスを発行するだけであるということである。「信頼」を築くために、ＤＲＭシステムには「ブラック・ボックス」が装備され

ており、これがこのようなＤＲＭシステムのために解読および暗号化機能を実行する。ブラック・ボックスは、公開／秘密鍵対、バージョン番号、および一意の署名を含み、これらは全て承認された証明機関によって供給される。公開鍵は、発行されたライセンスの一部を暗号化する目的でライセンス・サーバに使用可能とされ、これによってこのようなライセンスをこのようなブラック・ボックスに結び付ける。秘密鍵は、対応する公開鍵で暗号化した情報を解読する目的のために、ブラック・ボックスにのみ使用可能であり、ユーザやその他の誰にも使用できない。最初に、ＤＲＭシステムには公開／秘密鍵対を有するブラック・ボックスが供給され、ユーザが最初にライセンスを要求するときに、更新した保証ブラック・ボックスをブラック・ボックス・サーバからダウンロードするようにユーザに促す。ブラック・ボックス・サーバは、一意の公開／秘密鍵対と共に、更新ブラック・ボックスを供給する。このような更新ブラック・ボックスは、一意の実行可能コードで書かれており、ユーザの計算機上でのみ走り、定期的に再更新される。ユーザがライセンスを要求すると、クライアント・マシンはブラック・ボックス公開鍵、バージョン番号、および署名をライセンス・サーバに送り、そしてこのようなライセンス・サーバは、バージョン番号が現行であり署名が有効な場合、ライセンスを発行する。また、ライセンス要求は、ライセンスを要求するデジタル・コンテンツの識別、および要求したデジタル・コンテンツに関連する解読鍵を識別する鍵ＩＤも含む。ライセンス・サーバは、ブラック・ボックス公開鍵を用いて解読鍵を暗号化し、解読鍵を用いてライセンス条件を暗号化し、次いで暗号化した解読鍵および暗号化したライセンス条件を、ライセンス署名と共に、ユーザの計算機にダウンロードする。

【００１４】

一旦ダウンロードしたライセンスをＤＲＭシステムのライセンス・ストアに格納したなら、ユーザはライセンスによって与えられライセンス条件において指定された権利にしたがって、デジタル・コンテンツをレンダリングすることができる。デジタル・コンテンツをレンダリングする要求が行われると、ブラック・ボックスに解読鍵およびライセンス条件を解読させ、ＤＲＭシステムのライセンス評価部がこのようなライセンス条件を評価する。ブラック・ボックスは、ライセ

ンスの評価の結果、要求元にこのようなコンテンツを再生することを許可すると判断した場合にのみ、暗号化デジタル・コンテンツを解読する。解読したコンテンツは、レンダリング・アプリケーションに供給され、レンダリングが行われる。

（図面の簡単な説明）

前述の概要、および以下の本発明の実施形態の更に詳細な説明は、添付図面と関連付けて読むことにより、一層理解が深まるであろう。本発明を例示する目的のために、現在好適な実施形態を図面に示す。しかしながら、当然理解されるであろうが、本発明は図示する構成や手段そのものに限定される訳ではない。

（発明の詳細な説明）

図面を詳細に参照すると、全体を通じて同様のエレメントを示すために同様の番号が用いられている。図１には、本発明の一実施形態による実施アーキテクチャ１０を示す。概略的に、実施アーキテクチャ１０は、デジタル・コンテンツ１２の所有者にライセンス規則を指定させ、このライセンス規則を満たさなければ、ユーザの計算機１４上でこのようなデジタル・コンテンツ１２をレンダリングすることが許可されない。このようなライセンス規則は、デジタル・ライセンス１６に具体化され、ユーザ／ユーザの計算機１４（以後、このような用語は、特に状況が必要としない限り、相互交換可能とする）は、コンテンツ所有者またはその代理人から取得しなければならない。デジタル・コンテンツ１２は、暗号化した形態で配付され、自由に広く配付することもできる。好ましくは、デジタル・コンテンツ１２を解読するための解読鍵（ＫＤ）をライセンス１６と共に含ませる。

計算機環境

図１２および以下の論述は、本発明を実現するのに適した計算機環境の端的な一般的な説明を行なうことを意図している。必ずしもその必要はないが、本発明の説明は、少なくとも部分的には、プログラム・モジュールのような、クライアント・ワークステーションまたはサーバのようなコンピュータが実行する一般的なコンピュータ実行可能命令に関連して行なう。一般に、プログラム・モジュールは、ルーチン・プログラム、オブジェクト、コンポーネント、データ構造等を

含み、特定のタスクを実行したり、あるいは特定の抽象的データ・タイプを実装する。更に、本発明およびその一部は、ハンド・ヘルド・デバイス、マルチプロセッサ・システム、マイクロプロセッサ系電子機器またはプログラマブル消費者電子機器、ネットワークＰＣ、ミニコンピュータ、メインフレーム・コンピュータ等を含む、別のコンピュータ・システム構成でも実施可能であることも認めよう。また、本発明は、分散型計算機環境においても実施可能であり、この場合、通信ネットワークを通じてリンクされたリモート処理デバイスによってタスクを実行する。分散型計算機環境では、プログラム・モジュールは、ローカルおよびリモート・メモリ記憶装置双方に位置することができる。

【００１５】

図１２に示すように、本発明を実現する汎用計算機システムの一例は、従来のパーソナル・コンピュータ１２０等のを含む。このパーソナル・コンピュータ１２０は、演算装置１２１、システム・メモリ１２２、およびシステム・メモリから演算装置１２１までを含む種々のシステム・コンポーネントを結合するシステム・バス１２３を含む。システム・バス１２３は、数種類のバス構造のいずれでもよく、メモリ・バスまたはメモリ・コントローラ、周辺バス、および種々のバス構造のいずれかを用いてローカル・バスが含まれる。システム・メモリは、リード・オンリ・メモリ（ＲＯＭ）１２４およびランダム・アクセス・メモリ（ＲＡＭ）１２５を含む。基本入出力システム１２６（ＢＩＯＳ）は、起動中のように、パーソナル・コンピュータ１２０内のエレメント間におけるデータ転送を補助する基本的なルーティンを含み、ＲＯＭ１２４内に格納されている。

【００１６】

更に、パーソナル・コンピュータ１２０は、図示しないハード・ディスクの読み書きを行なうハード・ディスク・ドライブ１２７、リムーバブル磁気ディスク１２９の読み書きを行なう磁気ディスク・ドライブ１２８、ＣＤ－ＲＯＭまたはその他の光媒体のようなリムーバブル光ディスク１３１の読み書きを行なう光ディスク・ドライブ１３０のような種々の周辺ハードウエア・デバイスも含む。ハード・ディスク・ドライブ１２７、磁気ディスク・ドライブ１２８、および光ディスク・ドライブ１３０は、それぞれ、ハード・ディスク・ドライブ・インター

フェース１３２、磁気ディスク・ドライブ・インターフェース１３３、および光ドライブ・インターフェース１３４を介して、システム・バス１２３に接続されている。ドライブおよびそれに関連するコンピュータ読取可能媒体は、コンピュータ読取可能命令、データ構造、プログラム・モジュールおよびパーソナル・コンピュータ２０のその他のデータの不揮発性格納を行なう。

【００１７】

ここに記載する環境の一例は、ハード・ディスク、リムーバブル磁気ディスク１２９およびリムーバブル光ディスク１３１を採用するが、コンピュータによるアクセスが可能なデータを格納することができる、別の形式のコンピュータ読取可能媒体も、動作環境例では使用可能であることは、当業者には認められよう。このような他の形式の媒体は、磁気カセット、フラッシュ・メモリ・カード、デジタル・ビデオ・ディスク、ベルヌーイ・カートリッジ、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリ・メモリ（ＲＯＭ）等を含む。

【００１８】

ハード・ディスク、磁気ディスク１２９、光ディスク１３１、ＲＯＭ１２４またはＲＡＭ１２５上には、多数のプログラム・モジュールを格納可能であり、オペレーティング・システム１３５、１つ以上のアプリケーション・プログラム１３６、その他のプログラム・モジュール１３７、およびプログラム・データ１３８を含む。ユーザは、キーボード１４０およびポインティング・デバイス１４２のような入力デバイスによって、コマンドおよび情報をパーソナル・コンピュータ２０に入力することができる。他の入力デバイス（図示せず）は、マイクロフォン、ジョイスティック、ゲーム・パッド、衛星ディッシュ、スキャナ等を含むことができる。これらおよびその他の入力デバイスは、多くの場合、システム・バスに結合するシリアル・ポート・インターフェース１４６を介して、演算装置１２１に接続されるが、パラレル・ポート、ゲーム・ポートまたはユニバーサル・シリアル・バス（ＵＳＢ）のようなその他のインターフェースによって接続することも可能である。また、ビデオ・アダプタ１４８のような周辺ハードウエア・インターフェース・デバイスを介して、モニタ１４７またはその他の種類のディスプレイ装置もシステム・バス１２３に接続してある。モニタ１４７に加えて

、パーソナル・コンピュータは、典型的に、スピーカおよびプリンタのような、その他の周辺出力デバイス（図示せず）を含む。図１２のシステム例は、ホスト・アダプタ１５５、小型コンピュータ・システム・インターフェース（ＳＣＳＩ）バス１５６、およびＳＣＳＩバス１５６に接続されている外部記憶装置１６２も含む。

【００１９】

パーソナル・コンピュータ１２０は、リモート・コンピュータ１４９のような１つ以上のリモート・コンピュータへの論理接続を用いれば、ネットワーク環境においても動作可能である。リモート・コンピュータ１４９は、別のパーソナル・コンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア・デバイス、またはその他の共通ネットワーク・ノードとすることができ、典型的に、パーソナル・コンピュータ１２０に関して先に述べたエレメントの多くまたは全てを含むが、図１２にはメモリ記憶装置１５０のみを図示している。図１２に示す論理接続は、ローカル・エリア・ネットワーク（ＬＡＮ）１５１およびワイド・エリア・ネットワーク（ＷＡＮ）１５２を含む。このようなネットワーク環境は、会社全域に及ぶコンピュータ・ネットワーク、イントラネットおよびインターネットでは一般的である。

【００２０】

ＬＡＮネットワーク環境で用いる場合、パーソナル・コンピュータ１２０は、ネットワーク・インターフェースまたはアダプタ１５３を介してローカル・ネットワーク１５１に接続する。ＷＡＮネットワーク環境で用いる場合、パーソナル・コンピュータ１２０は、典型的に、モデム１５４、またはインターネットのようなワイド・エリア・ネットワーク５２を通じて通信を確立する、その他の手段を含む。モデム１５４は、内蔵型でも外付けでもよく、シリアル・ポート・インターフェース１４６を介してシステム・バス１２３に接続する。ネットワーク環境では、パーソナル・コンピュータ１２０に関して図示したプログラム・モジュールまたはその一部は、ローカルまたはリモートメモリ記憶装置に格納することもできる。尚、図示のネットワーク接続は一例であり、コンピュータ間に通信リンクを確立する別の手段も使用可能であることは認められよう。

アーキテクチャ

再度図１を参照すると、本発明の一実施形態において、アーキテクチャ１０は、前述のユーザの計算機１４だけでなく、オーサリング・ツール１８、コンテンツ鍵データベース２０、コンテンツ・サーバ２２、ライセンス・サーバ２４、およびブラック・ボックス・サーバ２５を含む。

アーキテクチャ－オーサリング・ツール１８

オーサリング・ツール１８は、コンテンツ所有者が１片のデジタル・コンテンツ１２を、本発明のアーキテクチャ１０と共に使用可能な形態にパッケージ化するために用いられる。即ち、コンテンツ所有者は、オーサリング・ツール１８に、デジタル・コンテンツ１２、ならびに当該デジタル・コンテンツ１２に付随する命令および／または規則、ならびにデジタル・コンテンツ１２をどのようにパッケージ化するかに関する命令および／または規則を供給する。すると、オーサリング・ツール１８は、暗号化／解読鍵にしたがって暗号化したデジタル・コンテンツ１２、およびデジタル・コンテンツ１２に付随する命令および／または規則を有するデジタル・コンテンツ・パッケージ１２ｐを生成する。

【００２１】

本発明の一実施形態では、オーサリング・ツール１８は、いくつかの異なるデジタル・コンテンツ１２のパッケージ１２ｐを連続して生成するように命令され、その各々が、異なる暗号化／解読鍵にしたがって暗号化された同じデジタル・コンテンツを有する。当然理解されようが、デジタル・コンテンツ１２が同じである数個の異なるパッケージ１２ｐを有することは、このようなパッケージ１２ｐ／コンテンツ１２（以後、特に状況が必要としない限り、単に「デジタル・コンテンツ１２）の配付を追跡する際に有用となり得る。このような配付追跡は、通常は必要でないが、デジタル・コンテンツ１２が不法に販売または放送された場合には、調査機関が用いることができる。

【００２２】

本発明の一実施形態では、デジタル・コンテンツ１２を暗号化する暗号化／解読鍵は、対称鍵であり、暗号化鍵が解読鍵（ＫＤ）にもなる。以下で更に詳しく論ずるが、このような解読鍵（ＫＤ）は、このようなデジタル・コンテンツ１２

のライセンス１６の一部として、隠された形態でユーザの計算機１４に配信される。好ましくは、各デジタル・コンテンツ１２片には、コンテンツＩＤが備えられており（または、各パッケージ１２ｐにはパッケージＩＤが備えられており）、各解読鍵（ＫＤ）は鍵ＩＤを有し、オーサリング・ツール１８によって、各デジタル・コンテンツ１２片毎に（または各パッケージ１２ｐ毎に）解読鍵（ｋＤ）、鍵ＩＤ、およびコンテンツＩＤ（またはパッケージＩＤ）を鍵コンテンツ・データベース２０に格納する。加えて、デジタル・コンテンツ１２に対して発行されるライセンス１６の種類、ならびにライセンス１６の各種類に対する条件（terms and conditions）に関するライセンス・データも、コンテンツ鍵データベース２０、またはその他のデータベース（図示せず）に格納することができる。好ましくは、ライセンス・データは、後に、状況およびマーケット条件の要求に応じて、コンテンツ所有者によって変更することができる。

【００２３】

使用においては、オーサリング・ツール１８には、とりわけ、次の項目を含む情報が供給される。

－パッケージ化するデジタル・コンテンツ１２

－必要であれば、用いる透かしおよび／または指紋の形式およびパラメータ、

－必要であれば、用いるデータ圧縮の形式およびパラメータ、

－用いる暗号化の形式およびパラメータ、

－必要であれば、用いるシリアル化の形式およびパラメータ、および

－デジタル・コンテンツ１２に伴う命令および／または規則。

【００２４】

公知のように、透かしとは、隠されたコンピュータ読み取り可能信号であり、識別子としてデジタル・コンテンツ１２に追加される。指紋とは、各インスタンス毎に異なる透かしのことである。当然理解されようが、インスタンスとは、一意であるデジタル・コンテンツ１２のバージョンである。いずれのインスタンスでも、そのコピーを多数作成することができ、いずれのコピーも特定のインスタンスを有する。デジタル・コンテンツ１２の特定のインスタンスが不法に販売または放送された場合、調査機関は、このようなデジタル・コンテンツ１２に付加

されている透かし／指紋にしたがって十中八九容疑者を特定することができる。

【００２５】

データ圧縮は、本発明の精神および範囲から逸脱することなく、適切な圧縮アルゴリズムであればそのいずれにしたがって実施することも可能である。例えば、．ｍｐ３または．ｗａｖ圧縮アルゴリズムを用いることができる。勿論、デジタル・コンテンツ１２は、既に圧縮状態であってもよく、この場合追加の圧縮は不要である。

【００２６】

デジタル・コンテンツ１２に伴うべき命令／および規則は、実際上、本発明の精神および範囲から逸脱することなく、適切であればあらゆる命令、規則、またはその他の情報を含むことができる。以下で論ずるが、このような付随する命令／規則／情報は、主にユーザおよびユーザの計算機１４によって、ライセンス１６を取得し、デジタル・コンテンツ１２をレンダリングするために用いられる。したがって、このような付随命令／規則／情報は、適切にフォーマットされたライセンス取得スクリプト等を含むことができる。これについては、以下で更に詳しく説明する。加えて、または代わりに、このような付随命令／規則／情報は、デジタル・コンテンツ１２のプレビューをユーザに与えるように設計した、「プレビュー」情報を含むこともできる。

【００２７】

次に、供給された情報を用いて、オーサリング・ツール１８は、デジタル・コンテンツ１２に対応する１つ以上のパッケージ１２ｐを生成する。各パケージ１２ｐは、次に、コンテンツ・サーバ２に格納され、世界中に配付される。

【００２８】

本発明の一実施形態において、図２をここで参照すると、オーサリング・ツール１８は、ダイナミック・オーサリング・ツール１８であり、入力パラメータを受け取る。これらは、オーサリング・ツール１８上で指定し、動作させることができる。したがって、このようなオーサリング・ツール１８は、多数片のデジタル・コンテンツ１２に対して、パッケージ１２ｐの多数の変形を迅速に生成することができる。好ましくは、入力パラメータは、図示のように、辞書２８の形態

で具体化する。ここで、辞書２８は、以下のようなパラメータを含む。

【００２９】

－デジタル・コンテンツ１２を有する入力ファイル２９ａの名称、

－行われるエンコードの形式、

－用いる暗号化／解読鍵（ＫＤ）、

－パッケージ１２ｐ内にデジタル・コンテンツ１２と共にパッケージ化する付随命令／規則／情報（「ヘッダ情報」）、

－行なわれる多重化（muxing）の形式、および

－デジタル・コンテンツ１２に基づくパッケージ１２ｐを書き込む出力ファイル２９ｂの名称。

【００３０】

当然理解されようが、このような辞書２８は、オーサリング・ツール１８のオペレータ（人間または機械）によって容易にかつ素早く変更可能であり、しがって、オーサリング・ツール１８によって実行するオーサリングの形式も、容易にかつ素早く、動的に変更可能である。本発明の一実施形態では、オーサリング・ツール１８は、コンピュータ画面上において人のオペレータに閲覧可能なオペレータ・インターフェース（図示せず）を含む。したがって、このようなオペレータは、インターフェースを通じて辞書２８を変更することができ、更にインターフェースによる辞書２８の変更を適切に補助したり、あるいは規制することも可能である。

【００３１】

オーサリング・ツール１８では、図２に見られるように、ソース・ファイル１８ａは、辞書２８からデジタル・コンテンツ１２を有する入力ファイル２９ａの名称を検索し、ＲＡＭのようなメモリ２９ｃにデジタル・コンテンツ１２を置く。エンコード・フィルタ１８ｂは、次に、メモリ２９ｃ内のデジタル・コンテンツ１２に対してエンコードを行い、入力フォーマットから、辞書２８において指定されているエンコード形式に応じた出力フォーマット（即ち、．ｗａｖから．ａｓｐ、．ｍｐ３から．ａｓｐ．等）にファイルを転送し、エンコードしたデジタル・コンテンツ１２をメモリ２９ｃ内に置く。図示のように、パッケージ化す

るデジタル・コンテンツ１２（例えば、音楽）は、．ｗａｖまたは．ｍｐ３フォーマットのような圧縮フォーマットで受け取られ、．ａｓｐ（アクティブ・ストリーミング・プロトコル）フォーマットのようなフォーマットに変換される。勿論、その他の入力および出力フォーマットも採用でき、本発明の精神および範囲から逸脱する訳ではない。

【００３２】

その後、暗号化フィルタ１８ｃがメモリ２９ｃ内のエンコード・デジタル・コンテンツ１２を、辞書２８において指定されている暗号化／解読鍵（ＫＤ）にしたがって暗号化し、暗号化したデジタル・コンテンツ１２をメモリ２９ｃ内に置く。次に、ヘッダ・フィルタ１８ｄが、辞書２８において指定されているヘッダ情報を、メモリ２９ｃ内の暗号化デジタル・コンテンツ１２に追加する。

【００３３】

当然理解されようが、状況に応じて、パッケージ１２ｐは、時間的に整合したデジタル・コンテンツ１２の多数のストリームを含む場合もある（１つのストリームを図２に示す）。このような多数のストリームは多重化されている（即ち「ｍｕｘｅｄ」）。したがって、多重化フィルタ１８ｅは、辞書２８において指定されている多重化形式にしたがって、メモリ２９ｃ内のヘッダ情報および暗号化デジタル・コンテンツ１２の多重化を行い、その結果をメモリ２９ｃに置く。次に、ファイル書き込みフィルタ１８ｆが、メモリ２９ｃからこの結果を検索し、このような結果を、パッケージ１２ｐとして辞書２８に指定されている出力ファイル２９ｂに書き込む。

【００３４】

尚、ある状況においては、実行するエンコードの形式は通常では変更しないことを注記しておく。多重化形式は典型的にエンコード形式に基づくので、多重化形式も通常では同様に変更しない。実際にそういう場合には、辞書２８は、エンコード形式および多重化形式に関するパラメータを含む必要はない。代わりに、エンコード形式をエンコード・フィルタに「ハードワイヤ」し、あるいは多重化形式を多重化フィルタに「ハードワイヤ」するだけでよい。勿論、状況が要求する場合には、オーサリング・ツール１８は前述のフィルタ全てを含まなくてもよ

く、あるいは他のフィルタを含んでもよく、含んだフィルタは、ハードワイヤにしても、辞書２８内で指定されているパラメータにしたがってその機能を実行してもよく、全て本発明の精神および範囲から逸脱することはない。

【００３５】

好ましくは、オーサリング・ツール１８は、適切なソフトウエアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような計算機およびこのようなソフトウエアの構造および動作は、ここの開示に基づけば明白なはずであり、したがって本開示において更に詳しい論述は必要でない。

アーキテクチャーコンテンツ・サーバ２２

再度図１を参照すると、本発明の一実施形態において、コンテンツ・サーバ２２は、オーサリングツール１８が生成したパッケージを配布するか、またはその他の方法で検索できるようにする。このようなパケージ１２ｐは、適切な配布チャネルのいずれかを通じて、コンテンツ・サーバ２２の要求に応じて配布することができ、本発明の精神および範囲から逸脱することはない。例えば、このような配布チャネルは、インターネットまたはその他のネットワーク、電子掲示板、電子メール等とすることもできる。加えて、コンテンツ・サーバ２２を用いて、パッケージ１２ｐを磁気または光ディスクあるいはその他の記憶装置にコピーすることもでき、このような記憶装置を配付してもよい。

【００３６】

尚、コンテンツ・サーバ２２は、いずれの信頼またはセキュリティ問題にも関係なく、パッケージを配布することは認められよう。以下で論ずるが、このような問題は、ライセンス・サーバ２４およびこのようなライセンス・サーバ２４とユーザの計算機１４との間の関係と関連付けて扱われる。本発明の一実施形態では、コンテンツ・サーバ２２は自由に、デジタル・コンテンツ１２を有するパッケージ１２ｐを、これを要求するあらゆる配布先にリリースし、配布する。しかしながら、コンテンツ・サーバ２２は、このようなパケージ１２ｐのリリースおよび配布に制約を設けることもでき、本発明の精神および範囲から逸脱する訳ではない。例えば、コンテンツ・サーバ２２は、配布前に、所定の配布料の支払を

最初に要求することもでき、あるいは配布先にそれ自体を同定することを要求することもでき、あるいは配布先の識別に基づいて配布を行なうか否か実際に判断することもできる。

【００３７】

加えて、コンテンツ・サーバ２２を用いて、オーサリング・ツール１８を制御することによって在庫管理を行い、予めある数の異なるパッケージ１２ｐを生成し、予測される需要を満たすようにすることもできる。例えば、サーバは、同じデジタル・コンテンツ１２に基づいて１００個のパッケージ１２ｐを生成し、各パッケージ１２ｐを１０回送達することもできる。パッケージ１２ｐの供給が例えば、２０に減少すると、コンテンツ・サーバ２２はオーサリング・ツール１８に、例えば、８０個の追加パッケージ１２ｐを再度生成するように指令することもできる。

【００３８】

好ましくは、アーキテクチャ１０内のコンテンツ・サーバ２２は、一意の公開／秘密鍵対（ＰＵ－ＣＳ，ＰＲ－ＣＳ）を有し、これをライセンス１６を評価し、対応するデジタル・コンテンツ１２を解読するための解読鍵（ＫＤ）を取得するプロセスの一部として採用する。これについては、以下で更に詳しく説明する。公知のように、公開／秘密鍵対は非対称鍵であり、鍵対における鍵の一方で暗号化されるものは、鍵対における鍵の他方を用いなければ解読することができない。公開／秘密鍵対暗号化システムでは、公開鍵は世界中に知らせることができるが、秘密鍵は、このような秘密鍵の所有者によって常に秘密に保持されていなければならない。したがって、コンテンツ・サーバ２２がその秘密鍵（ＰＲ－ＣＳ）でデータを暗号化する場合、解読の目的のためにその公開鍵（ＰＵ－ＣＳ）と共に、暗号化したデータを世界に送ることができる。対応して、外部デバイスがデータをコンテンツ・サーバ２２に送り、このようなコンテンツ・サーバ２２のみがこのようなデータを解読するようにしたい場合、このような外部デバイスは最初にコンテンツ・サーバ２２の公開鍵（ＰＵ－ＣＳ）を取得し、次いでこのような公開鍵でデータを暗号化しなければならない。したがって、コンテンツ・サーバ２２（そして、コンテンツ・サーバ２２のみ）がその秘密鍵（ＰＲ－ＣＳ

）を用いて、このような暗号化データを解読することができる。

【００３９】

オーサリング・ツール１８の場合と同様、コンテンツ・サーバ２２は、適切なソフトウエアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウエアの構造および動作は、ここの開示に基づいて明らかなはずであるので、本開示では詳細な説明は全く必要ない。更に、本発明の一実施形態では、オーサリング・ツール１８およびコンテンツ・サーバ２２は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。更に、コンテンツ・サーバ２２は、ある状況によっては、オーサリング・ツール１８を含み、先に論じたように、オーサリング・ツール１８の機能を実行する場合もあることは認められよう。

デジタル・コンテンツ・パッケージ１２ｐの構造

次に図３を参照すると、本発明の一実施形態において、コンテンツ・サーバ２２によって配布されるデジタル・コンテンツ・パッケージ１２ｐは次を含む。

【００４０】

－先に論じたように暗号化／解読鍵（ＫＤ）を用いて暗号化されたデジタル・コンテンツ（即ち、（ＫＤ（ＣＯＮＴＥＮＴ））、

－このようなデジタル・コンテンツ１２（またはパッケージ１２ｐ）のコンテンツＩＤ（またはパッケージＩＤ）、

－解読鍵（ＫＤ）の鍵ＩＤ、

－好ましくは無暗号化形態のライセンス取得情報、および

－コンテンツ・サーバ２２の秘密鍵（ＰＲ－ＣＳ）によって署名された、コンテンツ・サーバ２２の公開鍵（ＰＵ－ＣＳ）を暗号化する鍵ＫＤ（即ち、（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））。

【００４１】

（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））に関して、このような項目は、デジタル・コンテンツ１２および／またはパッケージ１２ｐの妥当性検査に関係して用いられることは理解されよう。これについては以下で説明する。デジタル署名

を有する認証（以下を参照のこと）とは異なり、鍵（ＰＵ－ＣＳ）は（ＫＤ（ＰＵ－ＣＳ））を取得するには必要ではない。代わりに、鍵（ＰＵ－ＣＳ）は、単に解読鍵（ＫＤ）を適用するだけで取得される。一旦こうして取得すれば、このような鍵（ＰＵ－ＣＳ）は、署名（Ｓ（ＰＲ－ＣＳ））の有効性を検査するために用いることができる。

【００４２】

また、このようにオーサリング・ツール１８によって構築されるパッケージ１２ｐに対して、このようなオーサリング・ツール１８は、恐らくは辞書２８から供給されるヘッダ情報として、既にライセンス取得情報および（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を所持していなければならない。更に、オーサリング・ツール１８およびコンテンツ・サーバ２２は、恐らくは（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を構築するために相互作用を行なわなければならない。このような相互作用は、例えば、次のステップを含む。

【００４３】

－コンテンツ・サーバ２２が（ＰＵ－ＣＳ）をオーサリング・ツール１８に送る。

－オーサリング・ツール１８が（ＫＤ）を用いて（ＰＵ－ＣＳ）を暗号化し、（ＫＤ（ＰＵ－ＣＳ））を生成する。

【００４４】

－オーサリング・ツール１８が（ＫＤ（ＰＵ－ＣＳ））をコンテンツ・サーバ２２に送る。

－コンテンツ・サーバ２２が（ＰＲ－ＣＳ）を用いて（ＫＤ（ＰＵ－ＣＳ））に署名し、（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））を生成する。

【００４５】

－コンテンツ・サーバ２２が（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））をオーサリング・ツール１８に送る。

アーキテクチャーライセンス・サーバ２４

再度図１を参照すると、本発明の一実施形態において、ライセンス・サーバ２４は、１片のデジタル・コンテンツ１２に関して、ユーザの計算機１４からライ

センス１６の要求を受信し、ユーザの計算機１４が、発行するライセンス１６を授かることについて信用できるか否か判定を行い、このようなライセンス１６を交渉し、このようなライセンス１６を作成し、このようなライセンス１６をユーザの計算機１４に送る機能を実行する。好ましくは、このように送信されるライセンス１６は、デジタル・コンテンツ１２を解読するための解読鍵（ＫＤ）を含む。このようなライセンス・サーバ２４およびこのような機能については、以下で更に詳しく説明する。好ましくは、そしてコンテンツ・サーバ２２と同様に、アーキテクチャ１０におけるライセンス・サーバ２４は、一意の公開／秘密鍵対（ＰＵ－ＬＳ，ＰＲ－ＬＳ）を有し、ライセンス１６を評価するプロセスの一部としてこれを用い、対応するデジタル・コンテンツ１２を解読するための解読鍵（ＫＤ）を取得する。これについては、以下で更に詳しく説明する。

【００４６】

オーサリング・ツール１８およびコンテンツ・サーバ２２と同様、ライセンス・サーバ２４は、適切なソフトウエアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウエアの構造および動作は、ここの開示に基づいて明らかなはずであり、本開示においては詳細な論述は全く不要である。更に、本発明の一実施形態では、オーサリング・ツール１８および／またはコンテンツ・サーバ２２は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。

【００４７】

本発明の一実施形態では、ライセンス１６の発行に先立って、ライセンス・サーバ２４およびコンテンツ・サーバ２２は、代理契約等を行い、ライセンス・サーバ２４が実際に、コンテンツ・サーバ２２が配布するデジタル・コンテンツ１２の少なくとも一部について、ライセンス付与機関（licensing authority）であることに同意する。当然理解されようが、１つのコンテンツ・サーバ２２は、数個のライセンス・サーバ２４と代理契約を結ぶことができ、あるいは１つのライセンス・サーバ２４が数個のコンテンツ・サーバ２２と代理契約を結ぶこともでき、いずれも本発明の精神および範囲から逸脱する訳ではない。

【００４８】

好ましくは、ライセンス・サーバ２４は、実際にそれがコンテンツ・サーバ２２によって配布するデジタル・コンテンツ１２のライセンス１６を発行する代理権を有することを世界に示すことができる。こうすることによって、ライセンス・サーバ２４は、コンテンツ・サーバ２２に、ライセンス・サーバ２４の公開鍵（ＰＵ－ＬＳ）を送り、そしてコンテンツ・サーバ２２はライセンス・サーバ２４に、コンテンツ・サーバ２２の秘密鍵（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））によって署名したコンテンツとして、ＰＵ－ＬＳを含むデジタル認証を送ることが好ましい。当然理解されようが、このような認証におけるコンテンツ（ＰＵ－ＬＳ）は、コンテンツ・サーバ２２の公開鍵（ＰＲ－ＣＳ）を用いなければ、アクセスすることはできない。当然理解されようが、一般には、基礎となるデータのデジタル署名は、このようなデータの暗号化形態であり、このようなデータが偽造されていたり、あるいはその他の方法で変更されている場合、解読の際にこのようなデータと一致しない。

【００４９】

１片のデジタル・コンテンツ１２に関連するライセンス代理権として、そしてライセンス付与機能の一部として、ライセンス・サーバ２４は、このようなデジタル・コンテンツ１２のための解読鍵（ＫＤ）にアクセスできなければならない。したがって、ライセンス・サーバ２４は、このようなデジタル・コンテンツ１２（またはパッケージ１２ｐ）に対する解読鍵（ＫＤ）、鍵ＩＤ、およびコンテンツＩＤ（またはパッケージＩＤ）を有するコンテンツ鍵データベース２０にアクセスできることが好ましい。

アーキテクチャーブラック・ボックス・サーバ２６

更に図１を参照すると、本発明の一実施形態では、ブラック・ボックス・サーバ２６は、ユーザの計算機１４において、新たなブラック・ボックス３０をインストールし、アップデートする機能を実行する。以下で更に詳しく説明するが、ブラック・ボックス３０は、ユーザの計算機１４のために、暗号化および解読機能を実行する。また、以下で更に詳しく説明するが、ブラック・ボックス３０は、安全であり攻撃から保護されることを想定している。このようなセキュリティ

および保護は、少なくとも部分的に、ブラック・ボックス３０を、必要に応じてブラック・ボックス・サーバ２６によって新たなバージョンにアップグレードすることによって得られる。これについては、以下で更に詳しく説明する。

【００５０】

オーサリング・ツール１８、コンテンツ・サーバ２２、およびライセンス・サーバ２４の場合と同様、ブラック・ボックス・サーバ２６は、適切なソフトウエアによって、適切なコンピュータ、プロセッサ、またはその他の計算機上に実装する。このような機械およびこのようなソフトウエアの構造および動作は、ここの開示に基づいて明らかなはずであり、したがって本開示では詳細な論述は不要である。更に、本発明の一実施形態では、ライセンス・サーバ２４、オーサリング・ツール１８、および／またはコンテンツ・サーバ２２は、単一のコンピュータ、プロセッサ、またはその他の計算機上に、各々別個のワーク・スペースに常駐することもできる。しかし、セキュリティの目的上、ブラック・ボックス・サーバ２６を別個の機械に有する方が賢明であることを注記しておく。

アーキテクチャーユーザの計算機１４

次に図４を参照すると、本発明の一実施形態では、ユーザの計算機１４は、パーソナル・コンピュータ等であり、キーボード、マウス、画面、プロセッサ、ＲＡＭ、ＲＯＭ、ハード・ドライブ、フロッピ・ドライブ、ＣＤプレーヤ等のようなエレメントを有する。しかしながら、ユーザの計算機１４は、とりわけ、テレビジョンまたはモニタのような専用閲覧デバイス、ステレオまたはその他の音楽プレーヤのような専用オーディオ・デバイス、専用プリンタ等でもよく、本発明の精神および範囲から逸脱することはない。

【００５１】

１片のデジタル・コンテンツ１２のコンテンツ所有者は、ユーザの計算機１４が、このようなコンテンツ所有者が指定した規則を固守すること、即ち、求められた態様でレンダリングを許可するライセンス１６をユーザが取得しなければ、デジタル・コンテンツ１２をレンダリングしないことを信用しなければならない。好ましくは、ユーザの計算機１４は、このような計算機１４が、デジタル・コンテンツ１２に関連しユーザによって取得されたライセンス１６に具体化されて

いるライセンス規則にしたがってでなければ、デジタル・コンテンツ１２をレンダリングしないことを、コンテンツ所有者に対して履行することができる、信頼（trusted）コンポーネントまたは機構３２を備えなければならない。

【００５２】

ここで、信頼機構３２は、デジタル権利管理（ＤＲＭ）システム３２であり、ユーザが１片のデジタル・コンテンツ１２をレンダリングすることを要求したときにイネーブルされ、ユーザが、求められた態様でデジタル・コンテンツ１２をレンダリングするライセンス１６を有するか否か判定を行い、必要であれば、このようなライセンス１６の取得を実施し、ライセンス１６にしたがってユーザがデジタル・コンテンツ１２を再生する権利を有するか否か判定を行い、実際にユーザがこのようなライセンス１６に応じてこのような権利を有する場合、レンダリングの目的で、デジタル・コンテンツ１２を解読する。ユーザの計算機１４上でのＤＲＭシステム３２の内容および機能、およびアーキテクチャ１０との関係について、以下に説明する。

ＤＲＭシステム３２

ＤＲＭシステム３２は、ここに開示するアーキテクチャ１０と共に４つの主要な機能を実行する。（１）コンテンツの取得、（２）ライセンスの取得、（３）コンテンツのレンダリング、および（４）ブラック・ボックス３０のインストール／更新である。好ましくは、これらの機能のいずれもいつの時点でも実行することができるとよいが、これらの機能の一部は、デジタル・コンテンツ１２が既に取得されていることを要件とすることは認められよう。

ＤＲＭシステム３２－コンテンツ取得

ユーザおよび／またはユーザの計算機１４によるデジタル・コンテンツ１２の取得は、典型的に、比較的単純であり、概略的には、暗号化デジタル・コンテンツ１２を有するファイルを、ユーザの計算機１４上に置くことから成る。勿論、ここに開示するアーキテクチャ１０およびＤＲＭシステム３２と共に動作するためには、暗号化デジタル・コンテンツ１２が、デジタル・パッケージ１２ｐのように、このようなアーキテクチャ１０およびＤＲＭシステム３２に適した形態であることが必要である。これについては以下で説明する。

【００５３】

当然理解されようが、デジタル・コンテンツ１２は、コンテンツ・サーバ２２から直接的にまたは間接的に、いずれの方法でも取得可能であり、本発明の精神および範囲から逸脱することはない。例えば、このようなデジタル・コンテンツ１２は、インターネットのようなネットワークからダウンロードしたり、取得した光または磁気ディスク等に配したり、電子メール・メッセージ等の一部として受信したり、あるいは電子掲示板等からダウンロードすることができる。

【００５４】

このようなデジタル・コンテンツ１２は、一旦取得すると、計算機１４上で走るレンダリング・アプリケーション３４（以下で説明する）、およびＤＲＭシステム３２によって、取得したデジタル・コンテンツ１２がアクセス可能となるように、格納することが好ましい。例えば、デジタル・コンテンツ１２は、ユーザの計算機１４のハード・ドライブ（図示せず）上、または計算機１４にアクセス可能なネットワーク・サーバ（図示せず）上のファイルとして置くこともできる。デジタル・コンテンツ１２を光または磁気ディスク等に取得する場合、このようなディスクを、ユーザの計算機１４に結合されている適切なドライブ（図示せず）に装填するだけでよい。

【００５５】

本発明では、直接配布源としてのコンテンツ・サーバ２２からでも、また間接配布源としてのなんらかの仲介物からでも、デジタル・コンテンツ１２を取得するために特殊なツールを全く必要としないことを想定している。即ち、デジタル・コンテンツ１２は、他のあらゆるデータ・ファイルと同様に容易に取得することが好ましい。しかしながら、ＤＲＭシステム３２および／またはレンダリング・アプリケーション３４は、ユーザがデジタル・コンテンツ１２を取得するのを助けるように設計したインターフェース（図示せず）を含むこともできる。例えば、インターフェースは、デジタル・コンテンツ１２を探索するように特別に設計したウェブ・ブラウザを含むことができ、デジタル・コンテンツ１２のソースであることがわかっている既定のインターネット・ウェブ・サイト等にリンクする。

ＤＲＭシステム３２－コンテンツ・レンダリング、第１部

図５Ａを参照すると、本発明の一実施形態では、暗号化デジタル・コンテンツ１２が配布され、ユーザによって受信され、ユーザによって格納ファイルの形態で計算機１４上に置かれていると仮定し、ユーザは、レンダリング・コマンド上である変形（variation）を実行することによって、デジタル・コンテンツ１２をレンダリングしようとする（ステップ５０１）。例えば、このようなレンダリング・コマンドは、デジタル・コンテンツ１２を「再生」または「開く」要求として具体化することができる。計算機環境によっては、例えば、ワシントン州RedmondのMICROSOFT Corporationが販売する”MICROSOFT WINDOWS（登録商標）”オペレーティング・システムのように、このような再生またはオープン・コマンドは、デジタル・コンテンツ１２を表わすアイコン上で「クリック」することと同じ位簡単にすることができる。勿論、このようなレンダリング・コマンドのその他の実施形態も採用可能であり、本発明の精神および範囲から逸脱する訳ではない。一般に、このようなレンダリング・コマンドは、ユーザがデジタル・コンテンツ１２を有するファイルを開くか、走らせるか、実行する等を指令するときにはいつでも実行するように考慮することができる。

【００５６】

重要なことは、そして付加的に、このようなレンダリング・コマンドは、デジタル・コンテンツ１２を、印刷形態、視覚形態、聴覚形態等のような別の形態にコピーする要求として具体化できることにある。当然理解されようが、同じデジタル・コンテンツ１２を、コンピュータ画面上におけるように、１つの形態でレンダリングし、次いで印刷文書のように別の形態でレンダリングすることもできる。本発明では、各レンダリング形式は、ユーザがそうする権利を有する場合にのみ実行される。これについては以下で説明する。

【００５７】

本発明の一実施形態では、デジタル・コンテンツ１２は、拡張子で終わるファイル名を有するデジタル・ファイルの形態であり、計算機１４は、このような拡張子に基づいて、特定の種類のレンダリング・アプリケーション３４を実行することを決定することができる。例えば、ファイル名拡張子が、デジタル・コンテ

ンツ１２はテキスト・ファイルであることを示す場合、レンダリング・アプリケーション３４は、ワシントン州RedmondのMICROSOFT Corporationが販売する"MICROSOFT WORD"のようなワード・プロセッサの何らかの形態となる。同様に、ファイル名拡張子が、デジタル・コンテンツ１２はオーディオ、ビデオ、および／またはマルチメディア・ファイルであることを示す場合、レンダリング・アプリケーション３４は、同様にワシントン州RedmondのMICROSOFT Corporationが販売する"MICROSOFT MEDIA PLAYER"のような、マルチメディア・プレーヤの何らかの形態となる。

【００５８】

勿論、レンダリング・アプリケーションを決定する他の方法も採用することができ、本発明の精神および範囲から逸脱する訳ではない。一例としてに過ぎないが、デジタル・コンテンツ１２は、無暗号化形態のメタデータ（前述のヘッダ情報）を含むこともでき、この場合、メタデータは、このようなデジタル・コンテンツ１２をレンダリングするために必要なレンダリング・アプリケーション３４の形式に関する情報を含む。

【００５９】

好ましくは、このようなレンダリング・アプリケーション３４は、ファイル名に関連するデジタル・コンテンツ１２を試験し、このようなデジタル・コンテンツ１２が権利保護形態で暗号化されているか否か判定を行なう（ステップ５０３，５０５）。保護されていない場合、これ以上の面倒なく、デジタル・コンテンツ１２をレンダリングすることができる（ステップ５０７）。保護されている場合、レンダリング・アプリケーション３４は、暗号化デジタル・コンテンツ１２から、このようなデジタル・コンテンツ１２を再生するためにＤＲＭシステム３２が必要か否か判定を行なう。これに応じて、このようなレンダリング・アプリケーション３４は、ユーザの計算機１４に、ＤＲＭシステム３２をその上で走らせるように指令する（ステップ５０９）。次に、このようなレンダリング・アプリケーション３４はこのようなＲＤＭシステム３２をコールし、デジタル・コンテンツ１２を解読する（ステップ５１１）。以下で更に詳しく論ずるが、ＤＲＭシステム３２は、実際には、ユーザがこのようなデジタル・コンテンツ１２に対

する有効なライセンス１６、および有効なライセンス１６におけるライセンス規則にしたがってデジタル・コンテンツ１２を再生する権利を有する場合にのみ、デジタル・コンテンツ１２を解読する。好ましくは、一旦ＤＲＭシステム３２がレンダリング・アプリケーション３４によってコールされた場合、このようなＤＲＭシステム３２は、少なくとも、ユーザがこのようなデジタル・コンテンツ１２を再生する権利を有するか否か判定を行なう目的で、レンダリング・アプリケーション３４から制御を引き受ける（ステップ５１３）。

ＤＲＭシステム３２のコンポーネント

ライセンス評価部３６は、要求されたデジタル・コンテンツ１２に対応する１つ以上のライセンス１６を突き止め、このようなライセンス１６が有効であるか否か判定を行い、このような有効なライセンス１６におけるライセンス規則を見直し、見直したライセンス規則に基づいて、要求元のユーザが、とりわけ、求められた態様で、要求したデジタル・コンテンツ１２をレンダリングする権利を有するか否か判定を行なう。当然理解されようが、ライセンス評価部３６は、ＤＲＭシステム３２における信頼コンポーネント（trusted component）である。この開示では、「信頼」とは、信頼エレメントが、ライセンス１６における権利の記述にしたがってデジタル・コンテンツ１２の所有者の望みを遂行することをライセンス・サーバ２４（またはその他のあらゆる信頼する側のエレメント（trusting element）に納得させること、およびユーザがいずれの邪悪なまたはその他の目的のためにもこのような信頼エレメントを容易に変更できないことを意味する。

【００６０】

ライセンス評価部３６が実際にライセンス１６を適性に評価することを保証するため、そしてこのようなライセンス評価部３６が、ライセンス１６の実際の評価を迂回する目的でユーザが偽造またはそれ以外に変更されていないことを保証するために、このようなライセンス評価部３６は信頼されなければならない。したがって、ライセンス評価部３６は、保護または隠蔽された環境で走り、このようなライセンス評価部３６へのユーザのアクセスが拒否されるようにする。勿論、その他の保護対策も、ライセンス評価部３６に関して採用することができ、本

発明の精神および範囲から逸脱することはない。

ＤＲＭシステム３２のコンポーネント－ブラック・ボックス３０

主に、そして先に論じたように、ブラック・ボックス３０は、ＤＲＭシステム３２において暗号化および解読機能を実行する。即ち、ブラック・ボックス３０は、ライセンス評価部３６と共に動作し、ある情報をライセンス評価機能の一部として解読および暗号化する。加えて、一旦ライセンス評価部３６が、実際にユーザが求められた態様で要求デジタル・コンテンツ１２をレンダリングする権利を有すると判定したなら、ブラック・ボックス３０には、このようなデジタル・コンテンツ１２のために解読鍵（ＫＤ）が与えられ、このような解読鍵（ＫＤ）に基づいて、このようなデジタル・コンテンツ１２を解読する機能を実行する。

【００６１】

また、ブラック・ボックス３０もＤＲＭシステム３２における信頼コンポーネントである。即ち、ライセンス・サーバ２４は、ブラック・ボックス３０が、ライセンス１６におけるライセンス規則にしたがってのみ解読機能を実行することを信用しなければならず、更にライセンス１６の実際の評価を迂回するという邪悪な目的でユーザによって偽造またはそれ以外に変更された場合には、このようなブラック・ボックス３０は動作しないことも信用しなければならない。したがって、ブラック・ボックス３０も保護即ち隠蔽された環境で走り、ユーザはこのようなブラック・ボックス３０へのアクセスを拒否される。この場合も、ブラック・ボックス３０に関して他の保護対策を採用することもでき、本発明の精神および範囲から逸脱することはない。好ましくは、そしてコンテンツ・サーバ２２およびライセンス・サーバ２４と同様に、ＤＲンシステム３２におけるブラック・ボックス３０は、一意の公開／秘密鍵対（ＰＵ－ＢＢ，ＰＲ－ＢＢ）を有し、ライセンス１６を評価し、デジタル・コンテンツ１２を解読するための解読鍵（ＫＤ）を取得するプロセスの一部として用いられる。これについては、以下で更に詳しく説明する。

ＤＲＭシステム３２のコンポーネント－ライセンス・ストア３８

ライセンス・ストア３８は、ＤＲＭシステム３２が対応するデジタル・コンテンツ１２に対して受領したライセンス１６を格納する。ライセンス・ストア３８

自体は、信頼される必要はない。何故なら、ライセンス・ストア３８は単にライセンス１６を格納するだけに過ぎず、その各々は既に信頼コンポーネントとして組み込まれているからである。これについては以下で説明する。本発明の一実施形態では、ライセンス・ストア３８は、単に、ハード・ディスク・ドライブまたはネットワーク・ドライブのようなドライブのサブディレクトリである。しかしながら、ライセンス・ストア３８は、ＤＲＭシステム３２に比較的好都合な場所においてライセンス１６を格納する機能を実行する限りにおいて、本発明の精神および範囲から逸脱することなく、他のあらゆる形態で具体化することも可能である。

ＤＲＭシステム３２のコンポーネント－状態ストア４０

状態ストア４０は、現在または以前ライセンス・ストア３８にあったライセンス３８に対応する状態情報を維持する機能を実行する。このような状態情報は、ＤＲＭシステム３２が作成し、必要に応じて状態ストア４０に格納される。例えば、特定のライセンス１６が対応する１片のデジタル・コンテンツ１２の所定回数のレンダリングのみを許可する場合、状態ストア４０は、このようなライセンス１６に関して実際にレンダリングが何回行われたかに関する状態情報を維持する。状態ストア４０は、もはやライセンス・ストア３８にはないライセンス１６に関する状態情報を維持し続け、状態ストア４０から対応する状態ストア情報を削除する試みにおいて、ライセンス・ストア３８からライセンス１６を削除し、次いで同じライセンス１６を取得することが有利となるような状況を回避する。

【００６２】

また、状態ストア４０も、内部に格納されている情報が、ユーザに一層好ましい状態にはリセットされないことを保証するために、信頼されなければならない。したがって、状態ストア４０も同様に保護即ち隠蔽された環境で走り、このような状態ストア４０に対するユーザのアクセスが拒否されるようにする。この場合も、状態ストア４０に関して他の保護対策を勿論採用することができ、本発明の精神および範囲から逸脱することはない。例えば、状態ストア４０は、ＤＲＭシステム３２によって、暗号化形態で計算機１４上に格納してもよい。

ＤＲＭシステム３２－コンテンツ・レンダリング、第２部

再度図５Ａを参照し、本発明の一実施形態におけるコンテンツ・レンダリングについて再度論ずる。一旦ＤＲＭシステム３２が、コール元のレンダリング・アプリケーション３４から制御を引き受けたなら、このようなＤＲＭシステム３２は、ユーザが求められた態様で要求されたデジタル・コンテンツ１２をレンダリングする権利を有するか否か判定を行なうプロセスを開始する。即ち、ＤＲＭシステム３２は、ライセンス・ストアにおいて有効な授権ライセンス１６を突き止めるか（ステップ５１５，５１７）、あるいはライセンス・サーバ２４から有効な授権ライセンス（enabling license）１６を取得しようとする（即ち、以下で論じ図７に示すライセンス取得機能を実行する）。

【００６３】

第１ステップとして、そしてここで図６を参照して、このようなＤＲＭシステム３２のライセンス評価部３６は、ライセンス３８をチェックして、デジタル・コンテンツ１２に対応する１つ以上のライセンス１６を受信しているか否か確認する（ステップ６０１）。典型的に、ライセンス１６は、以下で論ずるように、デジタル・ファイルの形態となっているが、本発明の精神および範囲から逸脱することなくライセンス１６は他の形態でもよいことは認められよう。典型的に、ユーザは、このようなライセンス１６がなくてもデジタル・コンテンツ１２を受信するが、本発明の精神および範囲から逸脱することなく、対応するライセンス１６と共に、デジタル・コンテンツ１２を受信するようにしてもよいことも同様に認められよう。

【００６４】

図３に関連付けて先に論じたように、デジタル・コンテンツ１２の各片は、パッケージ１２ｐ内にあり、コンテンツＩＤ（またはパッケージＩＤ）がこのようなデジタル・コンテンツ１２（またはパッケージ１２ｐ）を識別し、鍵ＩＤが、暗号化デジタル・コンテンツ１２を解読する解読鍵（ＫＤ）を識別する。好ましくは、コンテンツＩＤ（またはパッケージＩＤ）および鍵ＩＤは、無暗号化形態である。したがって、そして具体的には、デジタル・コンテンツ１２のコンテンツＩＤに基づいて、ライセンス評価部３６は、このようなコンテンツＩＤの適用可能性の識別を収容するライセンス・ストア８において、あらゆるライセンス１

６を探す。尚、特にデジタル・コンテンツ１２の所有者がこのようなデジタル・コンテンツ１２に対して数種類の異なるライセンス１６を有し、ユーザがこのようなライセンス１６を多数個取得している場合、このようなライセンス１６が多数見つかる場合もあることを注記しておく。実際に、ライセンス評価部３６がライセンス・ストア３８において、要求されたデジタル・コンテンツ１２に対応するライセンス１６を全く発見できない場合、ＤＲＭシステム３２は、以下で説明するライセンス取得機能を実行する（図５のステップ５１９）。

【００６５】

ここで、ＤＲＭシステム３２が、１片のデジタル・コンテンツ１２をレンダリングするように要求されており、対応する１つ以上のライセンス１６がライセンス・ストア３８内にあると仮定する。本発明の一実施形態では、ここで、ＤＲＭシステム３２のライセンス評価部３６は続いて、このようなライセンス１６の各々について、このようなライセンス１６自体が有効か否か判定する（図６のステップ６０３および６０５）。好ましくは、そして具体的に、各ライセンス１１６は、当該ライセンス１６の内容２８に基づいたデジタル署名２６を含む。当然理解されようが、デジタル署名２６は、コンテンツ２８が偽造またはそれ以外に変更されている場合、ライセンス１６とは一致しない。したがって、ライセンス評価部３６は、デジタル署名２６に基づいて、コンテンツ２８が、ライセンス・サーバ２４から受け取った形態になっているか（即ち、有効か）否か、判定を行なうことができる。ライセンス・ストア３８において有効なライセンス１６が見つからない場合、ＤＲＭシステム３２は、以下で説明するライセンス取得機能を実行し、このような有効なライセンス１６を取得することができる。

【００６６】

１つ以上の有効なライセンス１６が見つかったと仮定すると、有効なライセンス１６各々について、ＤＲＭシステム３２のライセンス評価部３６は、次に、このような有効なライセンス１６が、望ましい態様で対応するデジタル・コンテンツ１２をレンダリングする権利をユーザに与えるか（即ち、授権するか）否か判定を行なう。即ち、ライセンス評価部３６は、要求元のユーザが要求したデジタル・コンテンツ１２を再生する権利を有するか否か、各ライセンス１６における

権利の記述に基づいて、更にユーザがデジタル・コンテンツ１２で何をしようとしているのかに基づいて判定を行なう。例えば、このような権利の記述は、ユーザに、デジタル・コンテンツ１２をサウンドにレンダリングすることは許可するが、解読してデジタル・コピーにレンダリングすることは許可しない。

【００６７】

当然理解されようが、各ライセンス１６における権利の記述は、いくつかの要因のいずれかに基づいて、ユーザがデジタル・コンテンツ１２を再生する権利を有するか否か指定する。要因には、ユーザが誰であるか、ユーザがどこにいるか、どの種類の計算機１１４をユーザが用いているか、どのレンダリング・アプリケーション３４がＤＲＭシステム３２をコールしているのか、日付、時間等が含まれる。加えて、権利の記述は、例えば、所定回数の再生、所定の再生時間にライセンス１６を限定することもできる。このような場合、ＤＲＭシステム３２は、ライセンス１６に関するあらゆる状態情報を参照しなければならない（即ち、何回デジタル・コンテンツ１２がレンダリングされたか、デジタル・コンテンツ１２がレンダリングされた総時間量等）。このような状態情報は、ユーザの計算機１４のＤＲＭシステム３２の状態ストア４０に格納されている。

【００６８】

したがって、ＤＲＭシステム３２のライセンス評価部３６は、有効な各ライセンス１６の権利の記述を検討し、このような有効なライセンス１６が、ユーザに求められた権利を授与するか否か判定を行なう。これを行なう際、ライセンス評価部３６は、ユーザの計算機１４内部の別のデータを参照して、ユーザが求めた権利を有するか否かの判定を実行しなければならない場合もある。図４に見られるように、このようなデータは、ユーザの計算機（機械）１４の識別４２およびその特定的な態様、ユーザの識別４４およびその特定的な態様、レンダリング・アプリケーション３４の識別およびその特定の態様、システム・クロック４６等を含むことができる。ユーザに求められた態様でデジタル・コンテンツ１２をレンダリングする権利を与える有効なライセンス１６が見つからない場合、ＤＲＭシステム３２は、次に、以下で説明するライセンス取得機能を実行し、実際にこのようなライセンス１６が取得可能であれば、このようなライセンス１６を取得

する。

【００６９】

勿論、場合によっては、ユーザは要求した態様でデジタル・コンテンツ１２をレンダリングする権利を取得できないこともある。何故なら、このようなデジタル・コンテンツ１２のコンテンツ所有者は、ユーザにテキスト文書を印刷したり、マルチメディア表現を無暗号化形態にコピーすることを許可するライセンス１６を付与しないことを指令している場合もあるからである。本発明の一実施形態では、デジタル・コンテンツ１２は、ライセンス１６の購入時にどんな権利が利用可能かに関するデータ、および利用可能なライセンス１６の種類を含む。しかしながら、１片のデジタル・コンテンツ１２のコンテンツ所有者は、いずれの時点においても、このようなデジタル・コンテンツ１２に対して得られるライセンス１６を変更することによって、このようなデジタル・コンテンツ１２に現在利用可能な権利を変更する可能性があることは認められよう。

ＤＲＭシステム３２－ライセンス取得

ここで図７を参照すると、実際にライセンス評価部３６がライセンス・ストア３８において、要求されたデジタル・コンテンツ１２に対応する有効な授権ライセンス１６を全く見つけられない場合、ＤＲＭシステム３２は、ライセンス取得機能を実行する。図３に示すように、デジタル・コンテンツ１２の各片は、このようなデジタル・コンテンツ１２をレンダリングするためのライセンス１６を取得するにはどうすればよいかに関する無暗号化形態の情報（即ち、ライセンス取得情報）と共にパッケージ化されている。

【００７０】

本発明の一実施形態では、このようなライセンス取得情報は、利用可能なライセンス１６の種類、および１つ以上の適切なライセンス・サーバ２４にアクセスすることができる１つ以上のインターネット・ウェブ・サイトまたはその他のサイト情報を（とりわけ）含むことができる。ここで、各ライセンス・サーバ２４は実際にデジタル・コンテンツ１２に対応するライセンス１６を発行することができる。勿論、ライセンスは、他の態様で取得することもでき、本発明の精神および範囲から逸脱する訳ではない。例えば、ライセンス１６は、電子掲示板にお

いてライセンス・サーバ２４から取得したり、あるいは自分自身でまたは磁気または光ディスク等のファイルという形態で正規のメールによって取得することもできる。

【００７１】

ライセンス１６を取得するための場所が、実際にネットワーク上のライセンス・サーバ２４であると仮定すると、ライセンス評価部３６は、ウェブ・サイトまたはその他のサイト情報に基づいてこのようなライセンス・サーバ２４に対してネットワーク接続を確立し、次いでこのように接続したライセンス・サーバ２４からライセンス１６の要求を送る（ステップ７０１、７０３）。即ち、一旦ＤＲＭシステム３２がライセンス・サーバ２４とコンタクトしたなら、このようなＤＲＭシステム３２は適切なライセンス要求情報３７をこのようなライセンス・サーバ２４に送信する。本発明の一実施形態では、このようなライセンス１６の要求情報３６は、とりわけ、次を含むことができる。

【００７２】

－ＤＲＭシステム３２のブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ）、

－ＤＲＭシステム３２のブラック・ボックス３０のバージョン番号、

ブラック・ボックス３０を認証した証明機関からのデジタル署名を含む認証書（認証書は実際に前述のブラック・ボックス３０の公開鍵およびバージョン番号を含むこともできる）、

－デジタル・コンテンツ１２（またはパッケージ１２ｐ）を識別するコンテンツＩＤ（またはパッケージＩＤ）、

－デジタル・コンテンツ１２を解読するための解読鍵（ＫＤ）を識別する鍵ＩＤ、

－要求されたライセンス１６の種類（実際に多数の種類が使用可能な場合）、

－デジタル・コンテンツ１２のレンダリングを要求したレンダリング・アプリケーション３４の種類等。

【００７３】

勿論、これらよりも多い量または少ない量のライセンス１６の要求情報３６を、ＤＲＭシステム３２によって、ライセンス・サーバ２４に送信することもでき

、本発明の精神および範囲から逸脱することはない。例えば、レンダリング・アプリケーション３４の種類に関する情報が必要ではない場合もあり、一方ユーザおよび／またはユーザの計算機１４に関して追加の情報が必要な場合もある。

【００７４】

一旦ライセンス・サーバ２４がＤＲＭシステム３２からライセンス１６の要求情報３６を受信したなら、ライセンス・サーバ２４は、信頼／認証およびその他の目的のために、いくつかのチェックを行なうとよい。本発明の一実施形態では、このようなライセンス・サーバ２４は、証明機関のデジタル署名を含む認証書をチェックし、これが偽造またはそれ以外に変更されていないか否か判定を行なう（ステップ７０５、７０７）。されている場合、ライセンス・サーバ２４は、要求情報３６に基づいてあらゆるライセンス１６を付与することを拒否する。また、ライセンス・サーバ２４は、判明した「悪い」ユーザおよび／またはユーザの計算機１４のリストを保持することもでき、更にリスト上にあるこのような悪いユーザおよび／または悪いユーザの計算機１４からの要求に基づいて、あらゆあるライセンス１６を付与するのを拒否することもできる。このような「悪人」リストは、いずれの適切な態様でもコンパイルすることができ、本発明の精神および範囲から逸脱することはない。

【００７５】

受信した要求およびそれに付随する情報に基づいて、特にライセンス要求情報におけるコンテンツＩＤ（またはパッケージＩＤ）に基づいて、ライセンス・サーバ２４はコンテンツ鍵データベース２０（図１）に問い合わせ、要求の基準であるデジタル・コンテンツ１２（またはパッケージ１２ｐ）に対応するレコードを突き止める。先に論じたように、このようなレコードは、このようなデジタル・コンテンツ１２に対する解読鍵（ＫＤ）、鍵ＩＤ、およびコンテンツＩＤを含む。加えて、このようなレコードは、デジタル・コンテンツ１２に発行するライセンス１６の種類、ならびにライセンス１６の各種類毎の条件に関するライセンス・データを収容することができる。あるいは、このようなレコードは、このような追加情報を有する場所へのポインタ、リンク、または参照を含むこともできる。

【００７６】

前述のように、多数の種類のライセンス１６を得ることができる。例えば、比較的小額のライセンス料では、限られた回数のレンダリングを許可するライセンス１６を得ることができる。比較的大きな額のライセンス料では、満期日まで無制限のレンダリングを許可するライセンス１６を得ることができる。更に高額のライセンス料では、満期日なしで無制限のレンダリングを許可するライセンスを得ることができる。実際には、あらゆる種類のライセンス条件を有するあらゆる種類のライセンス１６でも、ライセンス・サーバ２４によって考案し発行することもでき、本発明の精神および範囲から逸脱することはない。

【００７７】

本発明の一実施形態では、ライセンス１６の要求は、ライセンス・サーバ２４からユーザの計算機１４まで送信する際に、ウェブ・ページ等の助けによって行われる。好ましくは、このようなウェブ・ページは、ライセンス１６の要求の基準であるデジタル・コンテンツ１２に対してライセンス・サーバ２４から得られるあらゆる種類のライセンス１６に関する情報を含む。

【００７８】

本発明の一実施形態では、ライセンス１６を発行するのに先立って、ライセンス・サーバ２４は、ブラック・ボックス３０のバージョン番号をチェックし、このようなブラック・ボックス３０が比較的新しいか否か判定を行なう（ステップ７０９、７１１）。当然理解されようが、ブラック・ボックス３０は、安全であり、邪悪な目的（即ち、ライセンス１６なく不適正にデジタル・コンテンツ１２をレンダリングしたり、対応するライセンス１６の条件に外れている）のユーザからの攻撃から保護することを目的とする。しかしながら、実際にはこのような攻撃から完全に安全なシステムもソフトウエアもないことは認められよう。

【００７９】

当然理解されようが、ブラック・ボックス３０が比較的新しい場合、即ち、比較的最近取得または更新された場合、このようなブラック・ボックス３０がこのような邪悪なユーザによる攻撃を受けて成功する可能性は少ない。好ましくは、そして信頼問題として、ライセンス・サーバ２４が、比較的新しくないブラック

・ボックス３０のバージョン番号を含む要求情報を有するライセンス要求を受信した場合、このようなライセンス・サーバ２４は、対応するブラック・ボックス３０が現行バージョンにアップグレードされるまで、要求されたライセンス１６を発行することを拒否する。これについては以下で説明する。単純に言えば、ライセンス・サーバ２４は、このようなブラック・ボックス３０が比較的新しくなければ、このようなブラック・ボックス３０を信頼しない。

【００８０】

本発明のブラック・ボックス３０に関連して、「新しい」または「比較的新しい」という用語は、ブラック・ボックス３０の使用年数および利用度に基づいてブラック・ボックス３０に信頼を与える機能と一貫して、適切な意味を有することができ、本発明の精神および範囲から逸脱することはない。例えば、「新しい」は、年数にしたがって定義することができる（即ち、１か月未満）。別の例として、「新しい」は、ブラックボックス３０がデジタル・コンテンツを解読した回数に基づいて定義することもできる（即ち、解読が２００回未満）。更に、「新しい」は、各ライセンス・サーバ２４が設定する理念に基づくこともでき、この場合１つのライセンス・サーバ２４は別のライセンス・サーバとは異なる定義を「新しい」に対してすることもでき、更に、とりわけ、ライセンス１６が要求されるデジタル・コンテンツ１２に応じて、または要求されたライセンス１６の種類に応じて、ライセンス・サーバ２４は「新しい」を別個に定義することもできる。

【００８１】

ブラック・ボックス３０のバージョン番号またはこのようなブラック・ボックス３０のその他の指標が新しいことに、ライセンス・サーバ２４が納得したと仮定すると、ライセンス・サーバ２４は次にユーザとライセンス１６の条件を交渉する。あるいは、ライセンス・サーバ２４はユーザとライセンス１６の交渉を行い、このようなブラック・ボックス３０が新しいことを示すブラック・ボックス３０のバージョン番号にそれ自体が納得する（ステップ７１３、次いで７１１を実行する）。勿論、交渉の量は、発行するライセンス１６の種類、およびその他の要因によって異なる。例えば、ライセンス・サーバ２４が単に一括払い無制限

使用ライセンス１６を発行する場合、殆ど交渉を行なう必要はない。一方、ライセンス１６が、変動する価値、スライド制、区切り点、およびその他の詳細のような項目に基づく場合、このような項目および詳細は、ライセンス・サーバ２４およびユーザ間で、ライセンス１６を発行可能となる前に案出しなければならない場合もある。

【００８２】

当然理解されようが、状況によっては、ライセンスの交渉は、ユーザが更にライセンス・サーバ２４に情報を提供しなければならないこともあり得る（例えば、ユーザ、ユーザの計算機１４等に関する情報）。重要なことは、ライセンスの交渉は、とりわけ、ユーザおよびライセンス・サーバ２４が相互に受諾可能な支払手段（クレジット・アカウント、デビット・アカウント、郵送による小切手等）および／または支払方法（即時一括払い、ある時間期間の分割）を決定しなければならないことである。

【００８３】

一旦ライセンス１６の全ての条件について交渉を行い、ライセンス・サーバ２４およびユーザ双方が同意したなら（ステップ７１５）、ライセンス・サーバ２４がデジタル・ライセンス１６を生成する（ステップ７１９）。このように生成するライセンス１６は、少なくとも部分的に、ライセンス要求、ブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ）、およびコンテンツ鍵データベース２０から取得した要求の基準となるデジタル・コンテンツ１２に対する解読鍵（ＫＤ）に基づいている。本発明の一実施形態では、そして図８に見られるように、生成したライセンス１６は次を含む。

【００８４】

－ライセンス１６を適用するデジタル・コンテンツ１２のコンテンツＩＤ、

－恐らくは解読鍵（ＫＤ）（即ち、ＫＤ（ＤＲＬ））で暗号化されている、デジタル権利ライセンス（ＤＲＬ）４８（即ち、ライセンス評価部３６が問い合わせることができる所定の書式で書かれたライセンス１６の権利の記述即ち実際の条件）、

－ライセンス要求において受信したブラック・ボックス３０の公開鍵（ＰＵ－

ＢＢ）で暗号化したデジタル・コンテンツ１２に対する解読鍵（ＫＤ）（即ち（ＰＵ－ＢＢ（ＫＤ））。

【００８５】

－（ＫＤ（ＤＲＬ））および（ＰＵ－ＢＢ（ＫＤ））に基づき、ライセンス・サーバ２４の秘密鍵（即ち、（Ｓ（ＰＲ－ＬＳ））を用いて暗号化した、ライセンス・サーバ２４からのデジタル署名（認証書の添付なし）、および

－ライセンス・サーバ２４がコンテンツ・サーバ２２から以前に取得した認証書。このような認証書は、ライセンス・サーバ２４がコンテンツ・サーバ２２からのライセンス１６を発行する権限を有することを示す（即ち、（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））。

【００８６】

当然理解されようが、前述のエレメントおよび恐らくその他のエレメントも、デジタル・ファイルまたはその他の何らかの適切な形態にパッケージ化される。同様に当然理解されようが、ＤＲＬ４８またはライセンス１６における（ＰＵ－ＢＢ（ＫＤ））が偽造またはそれ以外に変更されている場合、ライセンス１６におけるデジタル署名（Ｓ（ＰＲ－ＬＳ））は一致せず、したがって、このようなライセンス１６は有効性が認められない。この理由のため、ＤＲＬは必ずしも前述のような暗号化形態（即ち、（ＫＤ（ＤＲＬ））である必要はないが、場合によってはこのような暗号化形態が望ましい場合もあり、したがって、本発明の精神および範囲から逸脱することなく、採用してもよい。

【００８７】

一旦デジタル・ライセンス１６の準備が終了すると、次にこのようなライセンス１６を要求元（即ち、ユーザの計算機１４上のＤＲＭシステム３２）（図７のステップ７１９）。好ましくは、ライセンス１６は、その要求が行われたのと同じ経路（即ち、インターネットまたはその他のネットワーク）を通じて送信するとよいが、他の経路を用いてもよく、本発明の精神および範囲から逸脱することはない。受信時に、要求元ＤＲＭ３２は、自動的に受信したデジタル・ライセンス１６をライセンス・ストア３８に置くことが好ましい（ステップ７２１）。

【００８８】

尚、ユーザの計算機１４は、場合によっては誤動作する場合もあり、このようなユーザの計算機１４上のＤＲＭシステム３２のライセンス・ストア３８に格納されているライセンス１６が検索不能となり、失われる場合もあり得ることは理解されよう。したがって、ライセンス・サーバ２４は、発行したライセンス１６のデータベース５０（図１）を保持し、ユーザに実際に再発行を受ける権利がある場合、このようなライセンス・サーバ２５が、ユーザに発行したライセンス１６のコピーを与えるかまたは再発行を行なう（以後、「再発行」）ようにすることが好ましい。ライセンス１６が検索不能となり失われるという前述の場合では、状態ストア４０に格納されており、このようなライセンス１６に対応する状態情報も失われる可能性もある。このように失われた状態情報は、ライセンス１６を再発行する際に考慮に入れなければならない。例えば、比較的短い時間期間の後に一定の割合に応じた形態で固定数のレンダリング・ライセンス１６を合法的に再発行し、比較的長い時間期間の後には全く再発行しないことも可能である。

ＤＲＭシステム３２－ブラック・ボックス３０のインストール／更新

先に論じたように、ライセンス１６を取得する機能の一部として、ライセンス・サーバ２４は、ユーザの計算機１４のＤＲＭシステム３２が、比較的新しくないブラック・ボックス３０、即ち、比較的古いバージョン番号を有するブラック・ボックス３０を有する場合、ユーザからのライセンス１６の要求を拒否することができる。このような場合、このようなＤＲＭシステム３２のブラック・ボックス３０を更新し、ライセンス取得機能が進行できるようにすることが好ましい。勿論、ブラック・ボックス３０は他の時点でも更新可能であり、本発明の精神および範囲から逸脱することはない。

【００８９】

好ましくは、ユーザの計算機１４上にＤＲＭシステム３２をインストールするプロセスの一部として、ブラック・ボックス３０の一意でない「ライト」（lite）バージョンを用意する。このような「ライト」ブラック・ボックス３０は、１片のデジタル・コンテンツ１２をレンダリングする前に、一意の正規バージョンにアップグレードする。当然理解されようが、各ＤＲＭシステム３２における各ブラック・ボックス３０が一意であれば、１つのブラック・ボックス３０へのセ

キュリティ侵害は、他のいずれのブラック・ボックス３０に対しても容易に繰り返すことはできない。

【００９０】

次に図９を参照すると、ＤＲＭシステム３２は、ブラック・ボックス・サーバ等から要求することによって、一意のブラック・ボックス３０を取得する（先に論じ、図１に示した通りである）（ステップ９０１）。典型的に、このような要求を行なうにはインターネットを用いるが、他のアクセス手段も採用でき、本発明の精神および範囲から逸脱することはない。例えば、ブラック・ボックス・サーバ２６への接続は、ローカルまたはリモートのいずれでも、直接接続とすることができる。１つの一意の非ライト・ブラック・ボックス３０から別の一意の非ライト・ブラック・ボックス３０へのアップグレードも、いずれの時点においても、例えば、ライセンス・サーバ２４がブラック・ボックス３０を新しくないと見なしたときのように、ＤＲＭシステム３２によって要求することができる。これは、先に論じた通りである。

【００９１】

その後、ブラック・ボックス・サーバ２６は、新たな一意のブラック・ボックス３０を生成する（ステップ９０３）。図３に見られるように、新たなブラック・ボックス３０の各々には、バージョン番号、および証明機関からのデジタル署名を有する認証書が備えられている。ライセンス取得機能との関連で先に論じたように、ブラック・ボックス３０のバージョン番号は、その相対的な使用期間（age）および／または使用を示す。同様にライセンス取得機能との関連で先に論じた、証明機関からのデジタル署名を有する認証書は、ライセンス・サーバ２４がブラック・ボックス３０を信頼するという、証明機関からの申し出即ち証拠機構である。勿論、ライセンス・サーバ２４は、証明機関がこのような認証書を、実際に信頼のおけるブラック・ボックス３０に発行することを信用する。実際には、ライセンス・サーバ２４が特定の証明機関を信頼せず、このような証明機関が発行するいずれの認証書も有効と認めることを拒絶する場合もあり得る。例えば、特定の証明機関が不正に認証書を発行しているパターンに関与していることが発覚した場合、信頼を得ることはできない。

【００９２】

好ましくは、そして先に論じたように、ブラック・ボックス・サーバ２６は、新たに生成した一意のブラック・ボックス３０を有する新たな一意の公開／秘密鍵対（ＰＵ－ＢＢ，ＰＲ－ＢＢ）を含む。好ましくは、ブラック・ボックス３０の秘密鍵（ＰＵ－ＢＢ)は、このようなブラック・ボックス３０のみからアクセス可能であり、このようなブラック・ボックス３０を含むＤＲＭシステム３２を有する計算機１４およびそのユーザを含めて、世界のその他からは隠されており、アクセスすることはできない。

【００９３】

あらゆる秘匿方式は、実際にこのような秘匿方式が世界から秘密鍵（ＰＵ－ＢＢ)を隠す機能を実行する限り、その殆どを用いることができ、本発明の精神および範囲から逸脱することはない。一例としてに過ぎないが、秘密鍵（ＰＵ－ＢＢ)をいくつかのサブコンポーネントに分割し、各サブコンポーネントを一意に暗号化し、異なる場所に格納してもよい。このような状況では、このようなサブアセンブリを完全に組み立てて完全な秘密鍵（ＰＵ－ＢＢ)を決して生成しないことが好ましい。

【００９４】

本発明の一実施形態では、このような秘密鍵（ＰＵ－ＢＢ)を暗号化するには、コードを用いる暗号化技術に従う。即ち、このような実施形態では、ブラック・ボックス３０の実際のソフトウエア・コード（または他のソフトウエア・コード）が暗号化鍵（複数の暗号化鍵）として用いられる。したがって、例えば、邪悪な目的でユーザによってブラック・ボックス３０のコード（またはその他のソフトウエア・コード）が偽造されたり、あるいは他の方法で変更された場合、このような秘密鍵（ＰＵ－ＢＢ)を解読することはできない。

【００９５】

新たなブラック・ボックス３０の各々は、新たな公開／秘密鍵対（ＰＵ－ＢＢ，ＰＲ－ＢＢ）と共に配信されるが、このような新たなブラック・ボックス３０には、ユーザの計算機１４上のＤＲＭシステム３２に以前に配信した古いブラック・ボックス３０からの古い公開／秘密鍵対へのアクセスも与えることが好まし

い（ステップ９０５）。したがって、アップグレードしたブラック・ボックス３０は、古い鍵対を用いて、古いデジタル・コンテンツ１２およびこのような古い鍵対にしたがって生成した、対応する古いライセンス１６にもアクセスすることができる。これについては、以下で更に詳しく論ずる。

【００９６】

好ましくは、ブラック・ボックス・サーバ２６が配信するアップグレードしたブラック・ボックス３０は、ユーザの計算機１４に密接に連結即ち関連付けられる。したがって、アップグレードしたブラック・ボックス３０は、邪悪な目的およびその他のために、多数の計算機間で動作可能に転送することはできない。本発明の一実施形態では、ブラック・ボックス３０の要求（ステップ９０１）の一部として、ＤＲＭシステム３２は、このようなＤＲＭシステム３２に一意の、および／またはユーザの計算機１４に一意のハードウエア情報を、ブラック・ボックス・サーバ２６に提供し、ブラック・ボックス・サーバ２６は、部分的にこのような提供されたハードウエア情報に基づいて、ＤＲＭシステム３２にブラック・ボックス３０を生成する。このように生成されたアップグレード・ブラック・ボックス３０は、次にユーザの計算機１４に配信され、ＤＲＭシステム３２にインストールされる（ステップ９０７、９０９）。アップグレードしたブラック・ボックス３０が何らかの方法で別の計算機１４に転送された場合、転送されたブラック・ボックス３０は、このような他の計算機１４を対象とするのではないことを認識し、このようなその他の計算機１４上でレンダリングを進める要求を全て許可しない。

【００９７】

一旦新たなブラック・ボックス３０がＤＲＭシステム３２にインストールされると、このようなＤＲＭシステム３２は、ライセンス取得機能またはその他のいずれかの機能を実行することができる。

ＤＲＭシステム３２－コンテンツ・レンダリング、第３部

次に図５Ｂを参照し、ここでライセンス評価部３６が少なくとも１つの有効なライセンス１６を発見し、このような有効なライセンス１６の少なくとも１つが、求められた態様で対応するデジタル・コンテンツ１２をレンダリングするため

に必要な権利（即ち、授権）をユーザに与えることがわかったと仮定すると、ライセンス評価部３６は、更に用いるためにこのようなライセンス１６の１つを選択する（ステップ５１９）。即ち、要求されたデジタル・コンテンツ１２をレンダリングするために、ライセンス評価部３６およびブラック・ボックス３０は、一体となってこのようなライセンス１６から解読鍵（ＫＤ）を取得し、ブラック・ボックス３０はこのような解読鍵（ＫＤ）を用いて、デジタル・コンテンツ１２を解読する。本発明の一実施形態では、そして先に論じたように、ライセンス１６から取得した解読鍵（ＫＤ）は、ブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ（ＫＤ））で暗号化されており、ブラック・ボックス３０は、それの秘密鍵（ＰＵ－ＢＢ）を用いて、このように暗号化されている解読鍵を解読し、解読鍵（ＫＤ）を生成する（ステップ５２１、５２３）。しかしながら、デジタル・コンテンツ１２の解読鍵（ＫＤ）を取得するその他の方法を用いてもよく、本発明の精神および範囲から逸脱することはない。

【００９８】

一旦ブラック・ボックス３０がデジタル・コンテンツ１２の解読鍵（ＫＤ）を有し、ライセンス評価部３６からデジタル・コンテンツ１２をレンダリングする許可を得たなら、制御をレンダリング・アプリケーション３４に戻すことができる（ステップ５２５、５２７）。本発明の一実施形態では、レンダリング・アプリケーション３４は次にＤＲＭシステム３２／ブラック・ボックス３０をコールし、暗号化デジタル・コンテンツ１２の少なくとも一部をブラック・ボックス３０に送出し、解読鍵（ＫＤ）にしたがって解読する（ステップ５２９）。ブラック・ボックス３０は、デジタル・コンテンツ１２の解読鍵（ＫＤ）に基づいてデジタル・コンテンツ１２を解読し、次いでブラック・ボックス３０は、解読したデジタル・コンテンツ１２を実際にレンダリングするために、レンダリング・アプリケーション３４に戻す（ステップ５３３、５３５）。レンダリング・アプリケーション３４は、暗号化デジタル・コンテンツ１２の一部またはデジタル・コンテンツ１２全体をブラック・ボックス３０に送り、本発明の精神および範囲から逸脱することなく、このようなデジタル・コンテンツ１２の解読鍵（ＫＤ）に基づいて解読することができる。

【００９９】

好ましくは、レンダリング・アプリケーション３４がデジタル・コンテンツ１２をブラック・ボックス３０に送り解読する場合、ブラック・ボックス３０および／またはＤＲＭシステム３２はこのようなレンダリング・アプリケーション３４の認証を行い、これが実際にＤＲＭシステム３２に最初に走らせるように要求したのと同じレンダリング・アプリケーションであることを確認する（ステップ５３１）。あるいは、レンダリングの承認が、ある種のレンダリング・アプリケーション３４に対するレンダリング要求に基づき、実際に他の種類のレンダリング・アプリケーション３４でレンダリングすることによって、不正に取得されたという可能性もあり得る。認証に成功し、デジタル・コンテンツ１２がブラック・ボックス３０によって解読されたと仮定すると、レンダリング・アプリケーション３４は解読されたデジタル・コンテンツ１２をレンダリングすることができる（ステップ５３３、５３５）。

鍵トランザクション・シーケンス

次に図１０を参照すると、本発明の一実施形態では、鍵トランザクション・シーケンスを実行して、要求された１片のデジタル・コンテンツ１２に対する解読鍵（ＫＤ）を取得し、ライセンス１６を評価する（即ち、図５Ａおよび図５Ｂのステップ５１５ないし５２３を実行する）。このシーケンスでは、主にＤＲＭシステム３２はライセンス１６から解読鍵（ＫＤ）を取得し、ライセンス１６およびデジタル・コンテンツ１２から得た情報を用いて、双方の有効性を認証即ち確認し、次いでライセンス１６が実際に求められた態様でデジタル・コンテンツ１２をレンダリングする権利を与えるか否か判定を行なう。与える場合、デジタル・コンテンツ１２をレンダリングすることができる。

【０１００】

図８に示すように、デジタル・コンテンツ１２の各ライセンス１６が次を含むことを念頭に入れ、

－ライセンス１６を適用するデジタル・コンテンツ１２のコンテンツＩＤ、

－恐らく解読鍵（ＫＤ）で暗号化されているデジタル権利ライセンス（ＤＲＬ）４８（即ち、ＫＤ（ＤＲＫ））。

【０１０１】

－ブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ）で暗号化されているデジタル・コンテンツ１２の解読鍵（ＫＤ）（即ち、（ＰＵ－ＢＢ（ＫＤ））、

－（ＫＤ（ＤＲＫ））および（ＰＵ－ＢＢ（ＫＤ））に基づいて、そしてライセンス・サーバ２４の秘密鍵で暗号化されている、ライセンス・サーバ２４からのデジタル署名（即ち、（Ｓ（ＰＲ－ＬＳ））、および

－ライセンス・サーバ２４が以前にコンテンツ・サーバ２２から取得した認証書（即ち、（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））、

更に、図３に示すように、デジタル・コンテンツ１２を有するパッケージ１２ｐが次を含むことも念頭に入れ、

－このようなデジタル・コンテンツ１２のコンテンツＩＤ、

ＫＤによって暗号化されているデジタル・コンテンツ１２（即ち、（ＫＤ（ＣＯＮＴＥＮＴ））、

－暗号化されていないライセンス取得スクリプト、および

－コンテンツ・サーバ２２の秘密鍵（ＰＲ－ＣＳ）によって署名されたコンテンツ・サーバ２２の公開鍵（ＰＵ－ＣＳ）を暗号化する鍵ＫＤ、

本発明の一実施形態では、鍵トランザクションの特定のシーケンスを、デジタル・コンテンツ１２のライセンス１６の特定の１つに関して実行する。このシーケンスは次の通りである。

【０１０２】

１．ライセンス１６からの（ＰＵ－ＢＢ（ＫＤ））に基づいて、ユーザの計算機１４上のＤＲＭシステム３２のブラック・ボックス３０はその秘密鍵（ＰＲ－ＢＢ）を適用し、（ＫＤ）を取得する（ステップ１００１）。（ＰＲ－ＢＢ（ＰＵ－ＢＢ（ＰＵ－ＢＢ（ＫＤ））＝（ＫＤ））。尚、重要なことは、ブラック・ボックス３０は、これ以上の面倒なく、ＫＤを用いてデジタル・コンテンツ１２を解読しようとすることも可能であることを注記しておく。このような信頼は、このようなライセンス・サーバ２４が、このようなブラック・ボックス３０の信ぴょう性を保証する、証明機関からの認証書に基づいて、ライセンス１６を発行したときに確立されている。したがって、最終ステップではなく最初のステップ

としてブラック・ボックス３０が解読鍵（ＫＤ）を取得しても、ＤＲＭシステム３２は、以下に説明するように、全てのライセンス１６の妥当性検査および評価機能を実行し続ける。

【０１０３】

２．デジタル・コンテンツ１２からの（ＫＤ（ＰＵ－ＣＳ）Ｓ（ＰＲ－ＣＳ））に基づいて、ブラック・ボックス３０は新たに取得した解読鍵（ＫＤ）を適用して（ＰＵ－ＣＳ）を取得する（ステップ１００３）。（ＫＤ（ＫＤ（ＰＵ－ＣＳ）＝（ＰＵ－ＣＳ））。加えて、ブラック・ボックス３０は、署名（Ｓ（ＰＲ－ＣＳ））に対して（ＰＵ－ＣＳ）を適用し、このような署名およびこのようなデジタル・コンテンツ１２／パッケージ１２ｐが有効であることを納得する（ステップ１００５）。有効でない場合、プロセスを中断し、デジタル・コンテンツ１２へのアクセスを拒否する。

【０１０４】

３．ライセンス１６からの（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－ＣＳ））に基づいて、ブラック・ボックス３０は、新たに取得したコンテンツ・サーバ２２の公開鍵（ＰＵ－ＣＳ）を適用し、認証書が有効であることを納得する（ステップ１００７）。これは、ライセンス１６を発行したライセンス・サーバ２４がコンテンツ・サーバ２２からの機関（authority）にそうさせ、次いで認証書の内容を検査して（ＰＵ－ＬＳ）を取得することを意味する（ステップ１００９）。有効でない場合、プロセスを中止し、ライセンス１６に基づくデジタル・コンテンツ１２へのアクセスを拒否する。

【０１０５】

４．ライセンス１６からの（Ｓ（ＰＲ－ＬＳ））に基づいて、ブラック・ボックス３０は、新たに取得したライセンス・サーバ２４の公開鍵（ＰＲ－ＬＳ）を適用して、ライセンス１６が有効であることを納得する（ステップ１０１１）。有効でない場合、プロセスを中止し、ライセンス１６に基づくデジタル・コンテンツ１２へのアクセスを拒否する。

【０１０６】

５．全ての妥当性検査ステップが成功し、ライセンス１６内のＤＲＬ４８が実

際に解読鍵（ＫＤ）で暗号化されていると仮定すると、ライセンス評価部３６は、既に取得してある解読鍵（ＫＤ）を、ライセンス１６から取得した（ＫＤ（ＤＲＬ））に適用し、ライセンス１６からライセンス条件を得る（即ちＤＲＬ４８）（ステップ１０１３）。勿論、ライセンス１６におけるＤＲＬ４８が実際に解読鍵（ＫＤ）で暗号化されていない場合、ステップ１０１３を省略してもよい。次に、ライセンス評価部３６は、ＤＲＬ４８を評価し、問い合わせを行い、ユーザの計算機１４がライセンス１６内のＤＲＬ４８に基づいて、求められた態様で対応するデジタル・コンテンツ１２をレンダリングする権利を有するか否か（即ち、ＤＲＬ４８が授権付与しているか否か）判定を行なう（ステップ１０１５）。ライセンス評価部３６が、このような権利が存在しないと判定した場合、プロセスを中止し、ライセンス１６に基づくデジタル・コンテンツ１２へのアクセスを拒否する。

【０１０７】

６．最後に、ライセンス１６の評価の結果、ユーザの計算機１４はＤＲＬ４８の条件に基づいて、求められた態様で対応するデジタル・コンテンツ１２をレンダリングする権利を有するという肯定的な判断が得られたと仮定すると、ライセンス評価部３６は、ブラック・ボックス３０が解読鍵（ＫＤ）にしたがって対応するデジタル・コンテンツ１２をレンダリングできることを、このようなブラック・ボックス３０に通知する。その後、ブラック・ボックス３０は解読鍵（ＫＤ）を適用し、パケージ１２ｐからのデジタル・コンテンツ１２を解読する（即ち、(KD（ＫＤ（ＣＯＮＴＥＮＴ））=（ＣＯＮＴＥＮＴ））（ステップ１０１７）。

【０１０８】

先に具体化した一連のステップは、ライセンス１６およびデジタル・コンテンツ１２間の交互動作即ち「ピンポン動作」を表わすことを注記するのは重要である。このようなピンポン動作によって、デジタル・コンテンツ１２を緊密にライセンス１６に結び付けることを保証し、デジタル・コンテンツ１２およびライセンス１６双方が適性に発行され有効な形態で存在する場合にのみ、妥当性検査および評価プロセスを行なうことができることを保証する。加えて、ライセンス１

６からのコンテンツ・サーバ２２の公開鍵（ＰＵ－ＣＳ）、および解読した形態でパッケージ１２ｐからデジタル・コンテンツ１２を得るには（そして、恐らく、解読した形態でライセンス１６からライセンス条件（ＤＲＬ４８）を得るためにも）同じ解読鍵（ＫＤ）が必要であるので、このような項目も緊密に結び付けられる。また、署名の妥当性検査によっても、デジタル・コンテンツ１２およびライセンス１６が、それぞれコンテンツ・サーバ２２およびライセンス・サーバ２４から発行された同じ形態であることを保証する。したがって、ライセンス・サーバ２４を迂回することによってデジタル・コンテンツ１２を解読することは、不可能ではないにしても困難であり、デジタル・コンテンツ１２またはライセンス１６を変更しそして解読することも、不可能ではないにしても困難である。

【０１０９】

本発明の一実施形態では、署名の妥当性検査、特にライセンス１６の署名の妥当性検査は、代わりに次のように行われる。図８に示すように、ライセンス・サーバ１６の秘密鍵（ＰＲ－ＬＳ）によって署名を暗号化するのではなく、各ライセンス１６の署名を、秘密ルート鍵（ＰＲ－Ｒ）（図示せず）によって暗号化する。この場合、各ＤＲＭシステム３２のブラック・ボックス３０は、秘密ルート鍵（ＰＲ－Ｒ）に対応する公開ルート鍵（ＰＵ－Ｐ）（これも図示せず）を含む。秘密ルート鍵（ＰＲ－Ｒ）は、ルート・エンティティだけがわかっており、ライセンス・サーバ２４は、このようなライセンス・サーバ２４がルート・エンティティを用いてライセンス１６を発行するように調整した場合にのみ、ライセンス１６を発行することができる。

【０１１０】

即ち、このような実施形態では、

１．ライセンス・サーバ２４がその公開鍵（ＰＲ－ＬＳ）をルート・エンティティに供給する。

【０１１１】

２．ルート・エンティティはこのようなライセンス・サーバ２４に、秘密ルート鍵（ＰＲ－Ｒ）によって暗号化されたライセンス・サーバ公開鍵（ＰＵ－ＬＳ）を戻す（即ち、（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））。

【０１１２】

３．次に、ライセンス・サーバ２４は、ライセンス・サーバの公開鍵（Ｓ（ＰＲ－ＬＳ））によって暗号化された署名を有するライセンス１６を発行し、更に、ルート・エンティティからの認証書をライセンスに添付する（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））。

【０１１３】

ＤＲＭシステム１８がこのように発行されたライセンス１７の妥当性を検査するために、ＤＲＭシステム１８は、

１．公開ルート鍵（ＰＵ－Ｒ）を、添付した認証書（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））に適用し、ライセンス・サーバ公開鍵（ＰＵ－ＬＳ）を取得し、

２．取得したライセンス・サーバ公開鍵（ＰＵ－ＬＳ）をライセンス１６の署名（ＰＲ－ＬＳ）に適用する。

【０１１４】

重要なこととして、ルート・エンティティが認証書（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））をライセンス・サーバ２４に供給することによって、このようなライセンス・サーバ２４にライセンス１６を発行する許可を与えるのと丁度同じように、このようなライセンス・サーバ２４は同様に認証書を第２のライセンス・サーバ２４に供給し（即ち、（ＣＥＲＴ（ＰＵ－ＬＳ２）Ｓ（ＰＲ－ＬＳ１））、これによって第２のライセンス・サーバにもライセンス１６を発行させることができることも認められてしかるべきである。今や明白であろうが、第２ライセンス・サーバが発行するライセンス１６は、第１認証書（ＣＥＲＴ（ＰＵ－ＬＳ１）Ｓ（ＰＲ－Ｒ））および第２認証書（ＣＥＲＴ（ＰＵ－ＬＳ２）Ｓ（ＰＲ－ＬＳ１））を含む。同様に、このようなライセンス１６は、第１および第２認証書のチェーンに従うことによって、有効性を認められる。勿論、チェーンの中に追加のリンクを加え、これらを通過するようにしてもよい。

【０１１５】

前述の署名妥当性検査プロセスの利点の１つとして、ルート・エンティティが定期的に秘密ルート鍵（ＲＰ－Ｒ）を変更することによって、同様に定期的に各

ライセンス・サーバ２４に新たな認証書（ＣＥＲＴ（ＰＵ－ＬＳ）Ｓ（ＰＲ－Ｒ））を取得させることができる点にある。重要なことは、このような新たな認証書を取得する要件として、各ライセンス・サーバがそれ自体をアップグレードする必要があるということである。ブラック・ボックス３０の場合と同様、ライセンス・サーバ２４が比較的新しい場合、即ち、比較的最近アップグレードされている場合、ライセンス・サーバ２４を攻撃して成功する可能性は低くなる。したがって、信頼の問題として、各ライセンス・サーバ２４は、署名妥当性検査プロセスのような適切なアップグレード推進機構を通じて定期的にアップグレードしなければならないようにすることが好ましい。勿論、他のアップグレード機構を採用することもでき、本発明の精神および範囲から逸脱することにはならない。

【０１１６】

勿論、秘密ルート鍵（ＰＲ－Ｒ）を変更する場合、各ＤＲＭシステム１８における公開ルート鍵（ＰＵ－Ｒ）も変更しなければならない。このような変更は、例えば、通常のブラック・ボックス３０のアップグレードの間に行なえばよく、あるいは実際にはブラック・ボックス３０のアップグレードを行なうことが必要となる場合もある。変更した公開ルート鍵（ＰＵ－Ｒ）は潜在的に、古い秘密ルート鍵（ＰＲ－Ｒ）に基づいて発行した古いライセンス１６に対する署名の妥当性検査と干渉する可能性もあるが、このような干渉は、アップグレードしたブラック・ボックス３０が古い公開ルート鍵（ＰＵ－Ｒ）全てを記憶しておくことを要求することによって、最少に抑えることができる。あるいは、このような干渉を最少に抑えるには、ライセンス１６に対する署名の検証を１回だけ行なえばよいようにしてもよい。例えば、ＤＲＭシステム１８のライセンス評価部３６によって、最初にこのようなライセンス１６を評価する。このような場合、署名の検証が行われたか否かに関する状態情報をコンパイルし、このような状態情報をＤＲＭシステム１８の状態ストア４０に格納するべきであろう。

デジタル権利ライセンス４８

本発明では、ライセンス評価部３６は、ライセンス１６の権利記述即ち条件としてデジタル権利ライセンス（ＤＲＬ）４８を評価し、このようなＤＲＬ４８が、求められた態様でデジタル・コンテンツ１２の対応する１片のレンダリングを

許可するか否か判定を行なう。本発明の一実施形態では、いずれかのＤＲＬ言語によって、ライセンサ（即ち、コンテンツ所有者）がＤＲＬ４８を書くことができる。

【０１１７】

当然理解されようが、ＤＲＬ４８を指定するには多くの方法がある。したがって、いずれのＤＲＬ言語においても、高い柔軟性を許容しなければならない。しかしながら、特定のライセンス言語でＤＲＬ４８の全ての面を指定することは非実用的であり、このような言語の著者が、個々のデジタル・ライセンサが望むライセンスの可能な態様全てを確認できるようにすることは可能性が非常に低い。更に、非常に洗練されたライセンス言語は不要の場合もあり、比較的単純なＤＲＬ４８を与えるライセンサにとっては障害となる場合もある。しかしながら、ＤＲＬ４８をどのように指定するかについてライセンサを不必要に制約してはならない。同時に、ライセンス評価部３６は、常に多数の具体的なライセンスに関する問題に対して、ＤＲＬ４８から回答を得ることができなければならない。

【０１１８】

ここで図１１を参照すると、本発明では、ＤＲＬ４８はいずれのライセンス言語でも指定することができるが、言語識別子即ちタグ５４を含む。ライセンス評価部３６は、ライセンス１６を評価し、次いで言語タグ５４を調べる暫定ステップを実行し、このような言語を識別し、次いで適切なライセンス言語エンジン５２を選択し、このように識別した言語のライセンス１６にアクセスする。当然理解されようが、このようなライセンス言語エンジン５２が存在し、ライセンス評価部３６にアクセス可能でなければならない。存在しない場合、言語タグ５４および／またはＤＲＬ４８は、このような言語エンジン５２を取得する場所５６（典型的にウェブ・サイト）を含むことが好ましい。

【０１１９】

典型的に、言語エンジン５２は、ハード・ドライブのような、ユーザの計算機１４のメモリに常駐する、実行可能ファイルまたは１組のファイルという形態を取る。言語エンジン５２は、ライセンス評価部３６がＤＲＬ４８に直接問い合わせを行なう際に補助し、ライセンス評価部３６は、仲介役として作用する言語エ

ンジン４８等を介して間接的にＤＲＬ４８に問い合わせを行なう。言語エンジン５２を実行すると、ＲＡＭのような、ユーザの計算機１４のメモリのワーク・スペースにおいて走る。しかしながら、言語エンジン５２はその他のいずれの形態でも用いることができ、本発明の精神および範囲から逸脱することはない。

【０１２０】

好ましくは、いずれの言語エンジン５２およびいずれのＤＲＬ言語も、ライセンス評価部３６が、ＤＲＬ４８によって回答されることを期待する、少なくともある数の具体的なライセンスに関する質問に対応するようにする。したがって、ライセンス評価部３６は、いずれの特定のＤＲＬ言語にも結び付けられていない。ＤＲＬ４８はいずれの適切なＤＲＬ言語でも書くことができ、新たなライセンス言語で指定されたＤＲＬ４８は、既存のライセンス評価部３６に、対応する新たな言語エンジン５２を取得させることによって、このようなライセンス評価部３６が採用することができる。

ＤＲＬ言語

ＤＲＬ言語の例を２つ、それぞれのＤＲＬ４８に具体化した場合について、以下に示す。最初の「簡単な」ＤＬＲ４８は、ライセンス属性を指定するＤＲＬ言語で書かれており、一方２番目の「スクリプト」ＤＲＬ４８は、ＤＲＬ４８に指定されているスクリプトにしたがって機能を実行することができるＤＲＬ言語で書かれている。ＤＲＬ言語で書かれている場合、各コード行の意味は、その言語規則（linguistics）および／または以下に続く属性の記述チャートに基づいて明らかなはずである。

単純なＤＲＬ４８

【０１２１】

【表１】

Simple DRL 48:

```
<LICENSE>
    <DATA>
        <NAME>Beastie Boy's Play</NAME>
        <ID>39384</ID>
        <DESCRIPTION>Play the song 3 times</DESCRIPTION>
        <TERMS></TERMS>
        <VALIDITY>
            <NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>
            <NOTAFTER>19980102 23:20:14Z</NOTAFTER>
        </VALIDITY>
        <ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE>
        <LICENSORSITE>http://www.foo.com</LICENSORSITE>
```

```
<CONTENT>
        <NAME>Beastie Boy's</NAME>
        <ID>392</ID>
        <KEYID>39292</KEYID>
        <TYPE>MS Encrypted ASF 2.0</TTYPE>
</CONTENT>
<OWNER>
        <ID>939KDKD393KD</ID>
        <NAME>Universal</NAME>
        <PUBLICKEY></PUBLICKEY>
</OWNER>
<LICENSEE>
        <NAME>Arnold</NAME>
        <ID>939KDKD393KD</ID>
        <PUBLICKEY></PUBLICKEY>
</LICENSEE>
<PRINCIPAL TYPE='AND'>
        <PRINCIPAL TYPE='OR'>
                <PRINCIPAL>
                        <TYPE>x86Computer</TYPE>
                        <ID>3939292939d9e939</ID>
                        <NAME>Personal Computer</NAME>
                        <AUTHTYPE>Intel Authenticated Boot PC
                        SHA-1 DSA512</AUTHTYPE>
                        <AUTHDATA>29293939</AUTHDATA>
                </PRINCIPAL>
                <PRINCIPAL>
                        <TYPE>Application</TYPE>
                        <ID>2939495939292</ID>
                        <NAME>Window's Media Player</NAME>
                        <AUTHTYPE>Authenticode SHA-
                        1</AUTHTYPE>
                        <AUTHDATA>93939</AUTHDATA>
                </PRINCIPAL>
        </PRINCIPAL>
        <PRINCIPAL>
                <TYPE>Person</TYPE>
                <ID>39299482010</ID>
                <NAME>Arnold Blinn</NAME>
                <AUTHTYPE>Authenticate user</AUTHTYPE>
                <AUTHDATA>\\redmond\arnoldb</AUTHDATA>
        </PRINCIPAL>
</PRINCIPAL>
```

```
            <DRLTYPE>Simple</DRLTYPE>  [the language tag 54]
            <DRLDATA>
                  <START>19980102 23:20:14Z</START>
                  <END>19980102 23:20:14Z</END>
                  <COUNT>3</COUNT>
                  <ACTION>PLAY</ACTION>
            </DRLDATA>
            <ENABLINGBITS>aaaabbbbccccdddd</ENABLINGBITS>
      </DATA>
      <SIGNATURE>
      <SIGNERNAME>Universal</SIGNERNAME>
            <SIGNERID>9382ABK3939DKD</SIGNERID>
            <HASHALGORITHMID>MD5</HASHALGORITHMID>
            <SIGNALGORITHMID>RSA 128</SIGNALGORITHMID>
            <SIGNATURE>xxxyyyxxxyyyxxxyyy</SIGNATURE>
            <SIGNERPUBLICKEY></SIGNERPUBLICKEY>
            <CONTENTSIGNEDSIGNERPUBLICKEY></CONTENTSIGNEDSI
            GNERPUBLICKEY>
      </SIGNATURE>
</LICENSE>
```

【０１２２】

【表２】

Script DRL 48:

```
<LICENSE>
      <DATA>
            <NAME>Beastie Boy's Play</NAME>
            <ID>39384</ID>
            <DESCRIPTION>Play the song unlimited</DESCRIPTION>
            <TERMS></TERMS>
            <VALIDITY>
                  <NOTBEFORE>19980102 23:20:14Z</NOTBEFORE>
                  <NOTAFTER>19980102 23:20:14Z</NOTAFTER>
            </VALIDITY>
            <ISSUEDDATE>19980102 23:20:14Z</ISSUEDDATE>
            <LICENSORSITE>http://www.foo.com</LICENSORSITE>
            <CONTENT>
                  <NAME>Beastie Boy's</NAME
                  <ID>392</ID>
                  <KEYID>39292</KEYID>
                  <TYPE>MS Encrypted ASF 2.0</TTYPE>
            </CONTENT>
            <OWNER>
                  <ID>939KDKD393KD</ID>
```

```
                <NAME>Universal</NAME>
                <PUBLICKEY></PUBLICKEY>
            </OWNER>
            <LICENSEE>
                <NAME>Arnold</NAME>
                <ID>939KDKD393KD</ID>
                <PUBLICKEY></PUBLICKEY>
            </LICENSEE>
            <DRLTYPE>Script</DRLTYPE>    [the language tag 54]
            <DRLDATA>
                function on_enable(action, args) as boolean
                    result = False
                    if action = "PLAY" then
                        result = True
                    end if
                    on_action = False
                end function
                ...
            </DRLDATA>
        </DATA>
        <SIGNATURE>
            <SIGNERNAME>Universal</SIGNERNAME>
            <SIGNERID>9382</SIGNERID>
            <SIGNERPUBLICKEY></SIGNERPUBLICKEY>
            <HASHID>MD5</HASHID>
            <SIGNID>RSA 128</SIGNID>
            <SIGNATURE>xxxyyyxxxyyyxxxyyy</SIGNATURE>
            <CONTENTSIGNEDSIGNERPUBLICKEY></CONTENTSIGNEDSI
            GNERPUBLICKEY>
        </SIGNATURE>
</LICENSE>
```

以上に指定した２つのＤＲＬにおいて、掲示した属性は、以下の記述およびデータ・タイプを有する。

【０１２３】

【表３】

属性	説明	データ・タイプ
Ｉｄ	ライセンスのＩＤ	ＧＵＩＤ
名称	ライセンスの名称	ストリング
コンテンツＩｄ	コンテンツのＩＤ	ＧＵＩＤ
コンテンツ鍵Ｉｄ	コンテンツの暗号化鍵のＩＤ	ＧＵＩＤ
コンテンツ名	コンテンツの名称	ストリング
コンテンツ・タイプ	コンテンツのタイプ	ストリング
所有者Ｉｄ	コンテンツの所有者のＩＤ	ＧＵＩＤ
所有者名	コンテンツの所有者の名前	ストリング
所有者公開鍵	コンテンツ所有者の公開鍵。これは、コンテンツ所有者のベース－６４エンコード公開鍵である	ストリング
ライセンシＩｄ	ライセンスを得る人のＩｄ。ヌルでもよい。	ＧＵＩＤ
ライセンシ名	ライセンスを得る人の名前。ヌルでもよい。	ストリング
ライセンシ公開鍵	ライセンシの公開鍵これは、ライセンシのベース－６４エンコード公開鍵である。ヌルでもよい。	ストリング
説明	人が読める単純なランセンスの説明	ストリング
条件	ライセンスの法的条件。これは法的文書（prose）を含むページへのポインタとすることもできる。	ストリング
有効性終了	ライセンス有効期間終了	日付
有効性発生	ライセンスの有効期間開始	日付
発行日	ライセンスを発行した日付	日付
ＤＲＬタイプ	ＤＲＬのタイプ。例は、”SIMPLE”または”SCRIPT”を含む。	ストリング
ＤＲＬデータ	ＤＲＬに特定なデータ	ストリング
許可ビット	これらのビットは、実際のコンテンツへのアクセスを許可するビットである。これらのビットの解釈は、アプリケーションに委ねられるが、典型的に、これはコンテンツ解読のための秘密鍵である。このデータはベース－６４エンコードされて	ストリング

	いる。これらのビットは、個々の機械の公開鍵を用いて暗号化されていることを注記しておく。	
署名者Ｉｄ	ライセンスに署名した人のＩＤ	ＧＵＩＤ
署名者名	ライセンスに署名した人の名前	ストリング
署名者公開鍵	ライセンスに署名した人の公開鍵。これは、署名者のベース－６４エンコード公開鍵である。	ストリング
コンテンツ署名署名者公開鍵	コンテンツ・サーバの秘密鍵によって署名されたライセンスに署名した人の公開鍵。この署名を検証する公開鍵は、コンテンツに暗号化されている。これは、ベース－６４エンコードされている。	ストリング
ハッシュＡｌｇＩｄ	ハッシュを生成するために用いるアルゴリズム。これは、"MD5"のようなストリングである。	ストリング
署名Ａｌｇ Ｉｄ	署名を生成するために用いるアルゴリズム。これは、"RSA128"のようなストリングである。	ストリング
署名	データの署名。これはベース－６４エンコード・データである。	ストリング

メソッド

先に論じたように、言語エンジン５２およびいずれのＤＲＬ言語も、ＤＲＬ４８が回答することをデジタル・ライセンス評価部３６が期待する、少なくともある数の特定的なライセンスに関する質問に対応することが好ましい。このような対応する質問を認識することは、本発明の精神および範囲から逸脱することなく、あらゆる質問を含むことができ、先にあげた２つのＤＲＬ４８の例において用いられる用語と一致し、本発明の一実施形態では、このような対応する質問または、以下のような、「メソッド」は「アクセス・メソッド」、「ＤＲＬメソッド」、および「使用許可メソッド」を含む。

アクセス・メソッド

アクセス・メソッドは、最上位の属性に対してＤＲＬ４８に問い合わせるために用いる

VARIANT QuaryAttribute（ＢＳＴＲ鍵）

有効な鍵は、各々BSTRバリアントを戻す、Licence.Name， License.Id， Content.Name， Content.Id， Content.Type，Ower.Name， Owner.Id， Owner.PublicKye， Licensee.Name， Licensee.Id， Licensee.PublicKey， Description，およびTerms、ならびに、各々Dateバリアントを戻すValidity.StartおよびValidity.Endを戻す。

ＤＲＬメソッド

以下のＤＲＬメソッドの実装は、各ＤＲＬ４８毎に異なる。ＤＲＬメソッドの多くは、'data'と称するバリアント・パラメータを含み、ＤＲＬ４８と一層進んだ情報を交信することを目的とする。これは主に今後の拡張性のためにある。

Boolean IsActivated（バリアント・データ）

このメソッドは、ＤＲＬ４８／ライセンス１６が活性化しているか否かを示すブール変数を戻す。活性化したライセンス１６の一例は、限定動作ライセンス１６であり、最初の再生のときに４８時間だけアクティブとなる。

Activate（バリアント・データ）

このメソッドは、ライセンス１６を活性化するために用いられる。一旦ライセンス１６が活性化されると、不活性化することはできない。

Variant QueryDRL（バリアント・データ）

このメソッドは、一層進んだＤＲＬ４８と通信するために用いられる。これは、主にＤＲＬ４８の特徴集合の今後の拡張性に関する。

Variant GetExpires（ＢＳＴＲアクション、バリアント・データ）

このメソッドは、投入したアクションに関するライセンス１６の満期日を戻す。戻り値がＮＵＬＬの場合、ライセンスは無期限であると見なされるか、または未だ活性化されていない等のために、未だ満期日を有していない。

Variant GetCount（ＢＳＴＲアクション、バリアント・データ）

このメソッドは、投入されたアクションの残り動作回数を戻す。ＮＵＬＬが戻

された場合、動作は無限回数実行することができる。

Boolean IsEnabled（ＢＳＴＲアクション、バリアント・データ）

このメソッドは、ライセンス１６が、現時点において要求されているアクションに対応するか否かについて示す。

Boolean IsSunk（ＢＳＴＲアクション、バリアント・データ）

このメソッドは、ライセンス１６に対して支払が行われたか否かについて示す。前金で支払が済んでいるライセンス１６はＴＲＵＥを戻し、一方使用時に料金を徴収するライセンス１６のように、前金で支払が済んでいないライセンス１６は、ＦＡＬＳＥを戻す。

【０１２４】

使用許可メソッド

これらのメソッドは、コンテンツを解読する際に用いるライセンス１６を許可するために用いられる。

Boolean Validate（ＢＳＴＲ鍵）

このメソッドはライセンス１６の妥当性を検査するために用いられる。終了した鍵は、ライセンス１６の署名の妥当性検査に用いる、対応のデジタル・コンテンツ１２の解読鍵（ＫＤ）（即ち、（ＫＤ（ＰＵ－ＢＢ））によって暗号化された、ブラック・ボックス３０の公開鍵（ＰＵ－ＢＢ）である。戻り値がＴＲＵＥである場合、ライセンス１６が有効であることを示す。戻り値がＦＡＬＳＥである場合無効を示す。

int OpenLicense 16（ＢＳＴＲアクション、ＢＳＴＲ鍵、バリアント・データ）

このメソッドは、解読した許可ビットにアクセスする準備のために用いられる。終了した鍵は、前述のように、（ＫＤ（ＰＵ－ＢＢ））である。戻り値が０の場合、成功を示す。他の戻り値を定義することができる。

BSTR GetDecryptedEnablingBits（ＢＳＴＲアクション、バリアント・データ）

Variant GetDecryptedEnablingBitsAsBinary （ＢＳＴＲアクション、バリアント・データ）

これらのメソッドは、解読した形態の許可ビットにアクセスするために用いられる。これが多数の理由のいずれかのために成功しなかった場合、ヌル・ストリ

ングまたはヌル・バリアントが戻される。

void CloseLicense 16（ＢＳＴＲアクション、バリアント・データ）

このメソッドは、終了したアクションを実行するために、許可ビットへのアクセスを解除するために用いられる。これが多数の理由のいずれかのために成功しなかった場合、ヌル・ストリングが戻される。

発見法

先に論じたように、同じ１片のデジタル・コンテンツ１２に対して多数のライセンス１６が存在する場合、ライセンス１６の１つを選択して用いなければならない。前述のメソッドを用いると、以下の発見法を実施してこのような選択を行なうことができる。即ち、１片のデジタル・コンテンツ１２に対してあるアクション（例えば、「再生」）を実行するためには、以下のステップを実行することができる。

【０１２５】

１．特定の１片のデジタル・コンテンツ１２に適用するライセンス１６全てを得る。

２．このようなライセンス１６に対してIsEnabled関数をコールすることによってアクションをイネーブルしない各ライセンス１６を削除する。

【０１２６】

３．このようなライセンス１６に対してIsActivatedをコールすることによってアクティブでない各ライセンス１６を削除する。

４．このようなライセンス１６に対してIsSunkをコールすることによって、前金で支払が済んでいない各ライセンスを削除する。

【０１２７】

５．いずれかのライセンス１６が残されている場合、これを用いる。再生回数制限ライセンス１６を用いる前に、特に再生回数無制限ライセンス１６に満期日がある場合、再生回数無制限ライセンスを用いる。いずれの時点においても、ユーザは、例え選択が価格効率的でないとしても、既に取得してある特定のライセンス１６を選択することが許されて当然である。したがって、ユーザは、恐らくＤＲＭシステム３２には明白でない判断基準に基づいて、ライセンス１６を選択

することができる。

【０１２８】

６．放置されているライセンス１６がある場合、それを示すステータスを戻す。すると、ユーザには、

使用可能であれば、前金で支払が済んでいないライセンス１６を用いる、

使用可能であれば、ライセンス１６を活性化する、および／または

ライセンス・サーバ２４からライセンス取得を実行する、

という選択肢が与えられる。

結論

本発明に関連して実行するプロセスを達成するために必要なプログラミングは、比較的単純であり、関連のあるプログラミング分野の人々には明白であるはずである。したがって、このようなプログラミングをここには添付しない。つまり、本発明を達成するためには、本発明の精神および範囲から逸脱することはなく、いずれの特定のプログラミングでも用いることができる。

【０１２９】

前述の説明では、本発明は、新規でかつ有用な実施アーキテクチャ１０から成り、デジタル・コンテンツ１２を制御し任意の形態でレンダリングまたは再生することを可能とし、このような制御は柔軟性があり、このようなデジタル・コンテンツ１２のコンテンツ所有者によって定義可能であることがわかる。また、本発明は、デジタル・コンテンツ１２が、たとえコンテンツ所有者の制御の下にない計算機１４上でレンダリングするにしても、コンテンツ所有者による指定通りにしかデジタル・コンテンツ１２をレンダリングしない、新規で有用なレンダリング環境の制御から成る。更に、本発明は、コンテンツ所有者が許可しない方法で、このような計算機１４のユーザが１片のデジタル・コンテンツ１２にアクセスしようとする試みに対してでさえ、このようなデジタル・コンテンツ１２に関して、このような計算機１４上でコンテンツ所有者の権利を実施する信頼コンポーネントから成る。

【０１３０】

尚、本発明の概念から逸脱することなく、上述の実施形態には変更も可能であ

ることは認められよう。したがって、本発明は、開示した特定の実施形態に限定されるのではなく、添付した特許請求の範囲によって規定される本発明の精神および範囲内の変更も包含することを意図することは理解されよう。

【図面の簡単な説明】

【図１】

本発明の一実施形態による実施アーキテクチャを示すブロック図である。

【図２】

本発明の一実施形態による図１のアーキテクチャのオーサリング・ツールのブロック図である。

【図３】

本発明の一実施形態による図１のアーキテクチャと共に用いるデジタル・コンテンツを有するデジタル・コンテンツ・パッケージのブロック図である。

【図４】

本発明の一実施形態による図１のユーザの計算機のブロック図である。

【図５】

図５Ａは本発明の一実施形態にしたがってコンテンツをレンダリングするための、図４の計算機のデジタル権利管理（ＤＲＭ）システムと共に実行するステップを示すフロー図である。

図５Ｂは本発明の一実施形態にしたがってコンテンツをレンダリングするための、図４の計算機のデジタル権利管理（ＤＲＭ）システムと共に実行するステップを示すフロー図である。

【図６】

本発明の一実施形態にしたがって、何らかの有効な権限付与ライセンスがあるか否か判定するために、図４のＤＲＭシステムと共に実行するステップを示すフロー図である。

【図７】

本発明の一実施形態にしたがってライセンスを取得するために、図４のＤＲＭシステムと共に実行するステップを示すフロー図である。

【図８】

本発明の一実施形態にしたがって図１のアーキテクチャと共に用いるデジタル使用許諾のブロック図である。

【図９】

本発明の一実施形態にしたがって新たなブラック・ボックスを取得するために、図４のＤＲＭシステムと共に実行するステップを示すフロー図である。

【図１０】

本発明の一実施形態にしたがってライセンスおよび１片のデジタル・コンテンツの妥当性を検査し、コンテンツをレンダリングするために、図４のＤＲＭシステムと共に実行する鍵トランザクション・ステップを示すフロー図である。

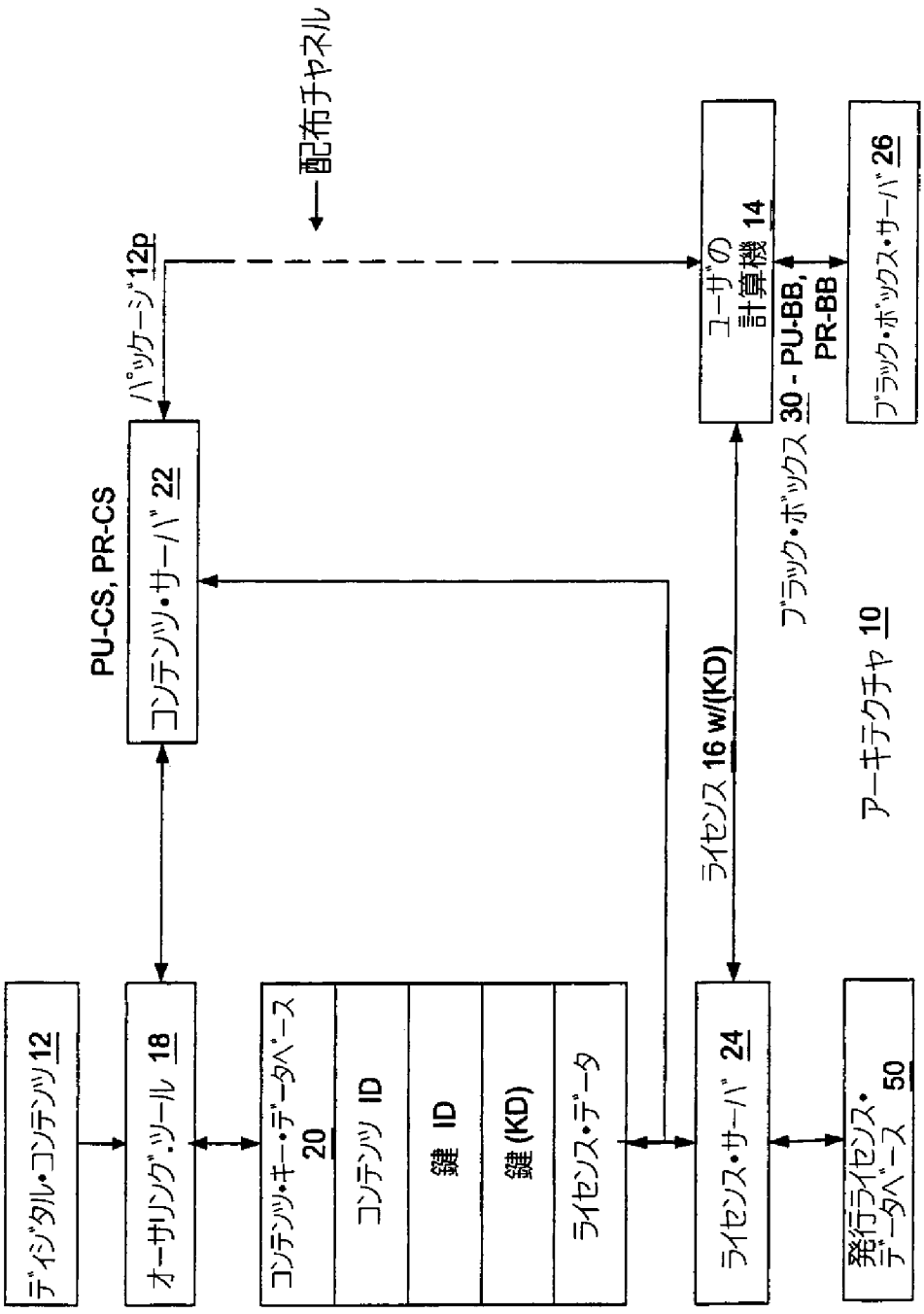
【図１１】

本発明の一実施形態によるライセンスのデジタル権利ライセンス（ＤＲＬ）、およびＤＲＭを解釈する言語エンジンと共に、図４のライセンス評価部を示すブロック図である。

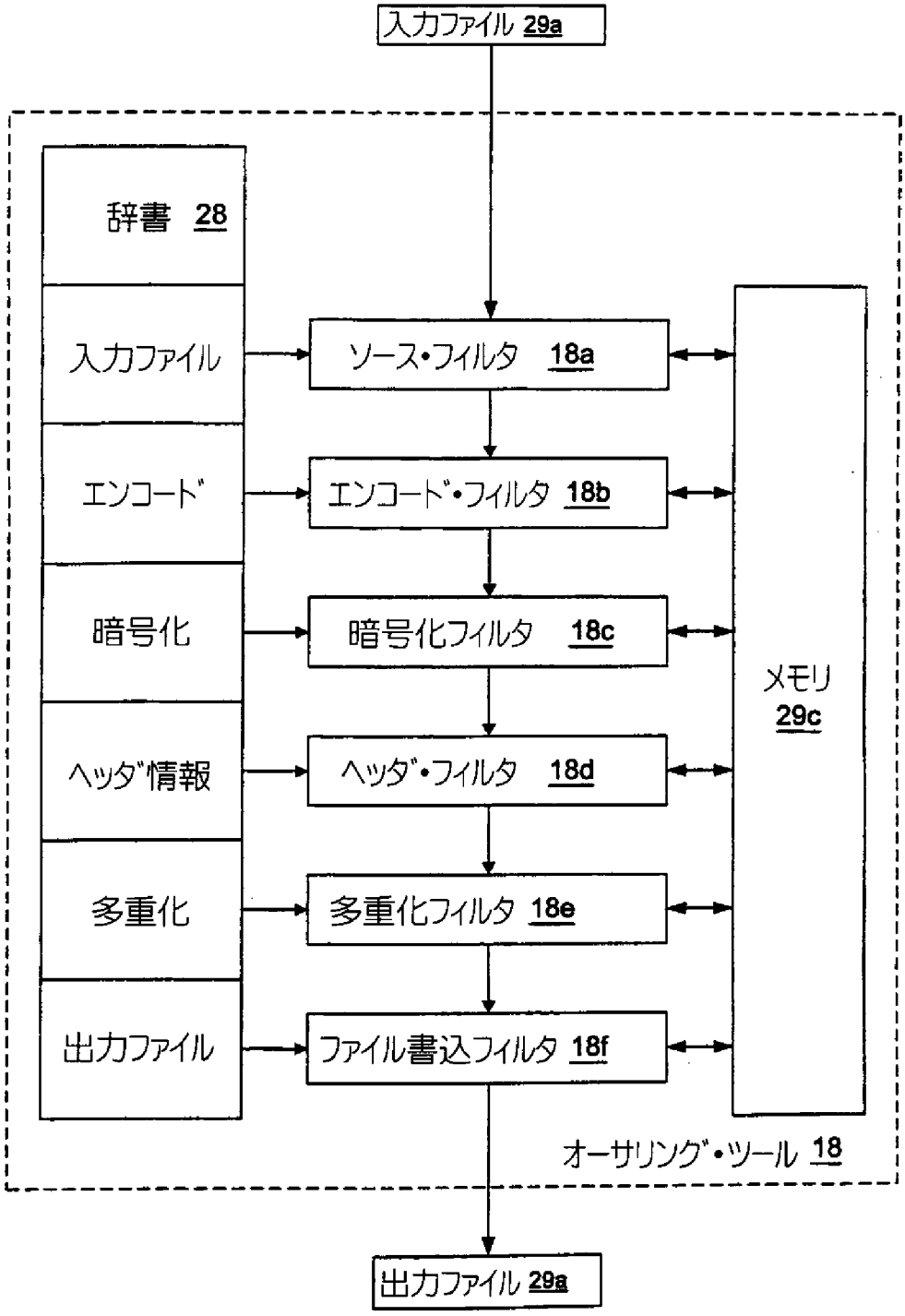
【図１２】

本発明の態様および／またはその一部を組み込むことができる汎用コンピュータ・システムを表わすブロック図である。

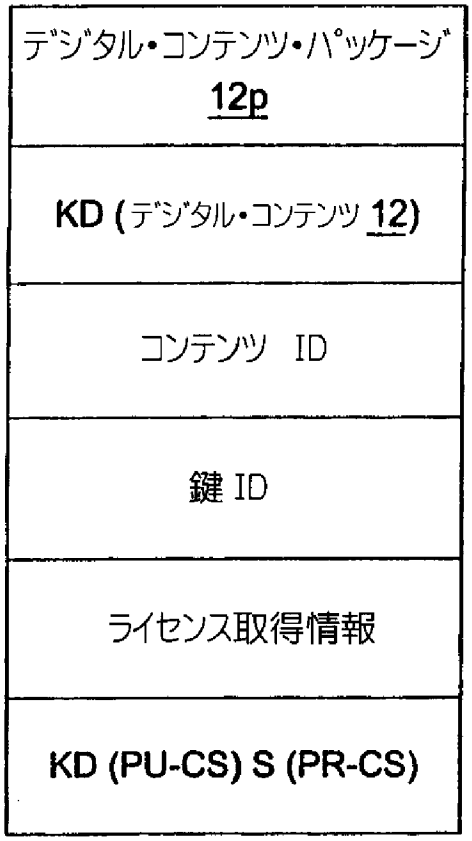
【図１】


配布チャネル
ユーザの計算機 14
ブラック・ボックス・サーバ 26
パッケージ 12p
PU-CS, PR-CS
コンテンツ・サーバ 22
ブラック・ボックス 30 - PU-BB, PR-BB
ライセンス 16 w/(KD)
アーキテクチャ 10
デジタル・コンテンツ 12
オーサリング・ツール 18
コンテンツ・キー・データベース 20
コンテンツ ID
鍵 ID
鍵 (KD)
ライセンス・データ
ライセンス・サーバ 24
発行ライセンス・データベース 50

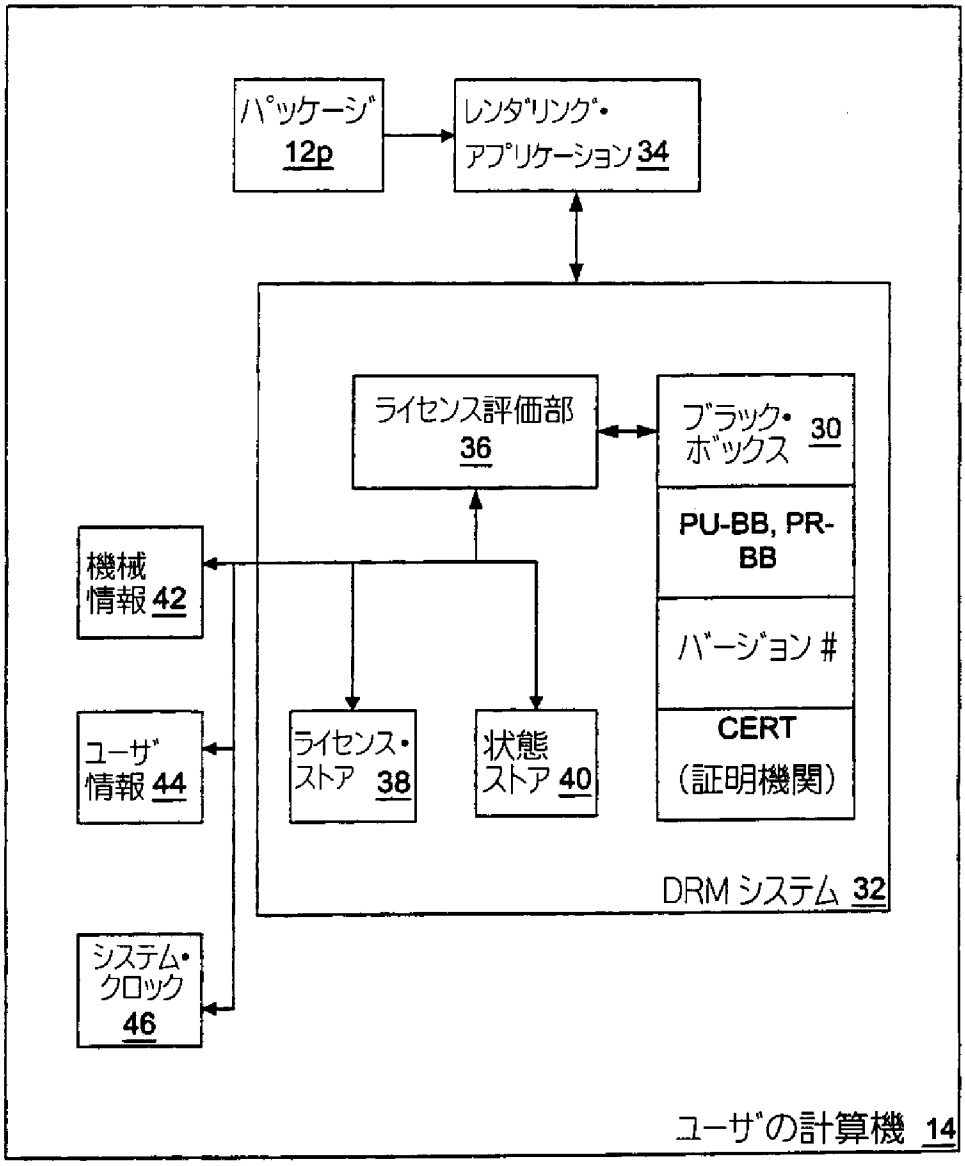
【図２】


入力ファイル 29a
辞書 28
入力ファイル
エンコード
暗号化
ヘッダ情報
多重化
出力ファイル
ソース・フィルタ 18a
エンコード・フィルタ 18b
暗号化フィルタ 18c
ヘッダ・フィルタ 18d
多重化フィルタ 18e
ファイル書込フィルタ 18f
メモリ 29c
オーサリング・ツール 18
出力ファイル 29a

【図３】


ﾃﾞｼﾞﾀﾙ・ｺﾝﾃﾝﾂ・ﾊﾟｯｹｰｼﾞ
12p
KD (ﾃﾞｼﾞﾀﾙ・ｺﾝﾃﾝﾂ 12)
コンテンツ ID
鍵 ID
ライセンス取得情報
KD (PU-CS) S (PR-CS)

【図４】


パッケージ 12p
レンダリング・アプリケーション 34
ライセンス評価部 36
ブラック・ボックス 30
PU-BB, PR-BB
バージョン #
CERT（証明機関）
機械情報 42
ユーザ情報 44
ライセンス・ストア 38
状態ストア 40
DRM システム 32
システム・クロック 46
ユーザの計算機 14

【図５Ａ】

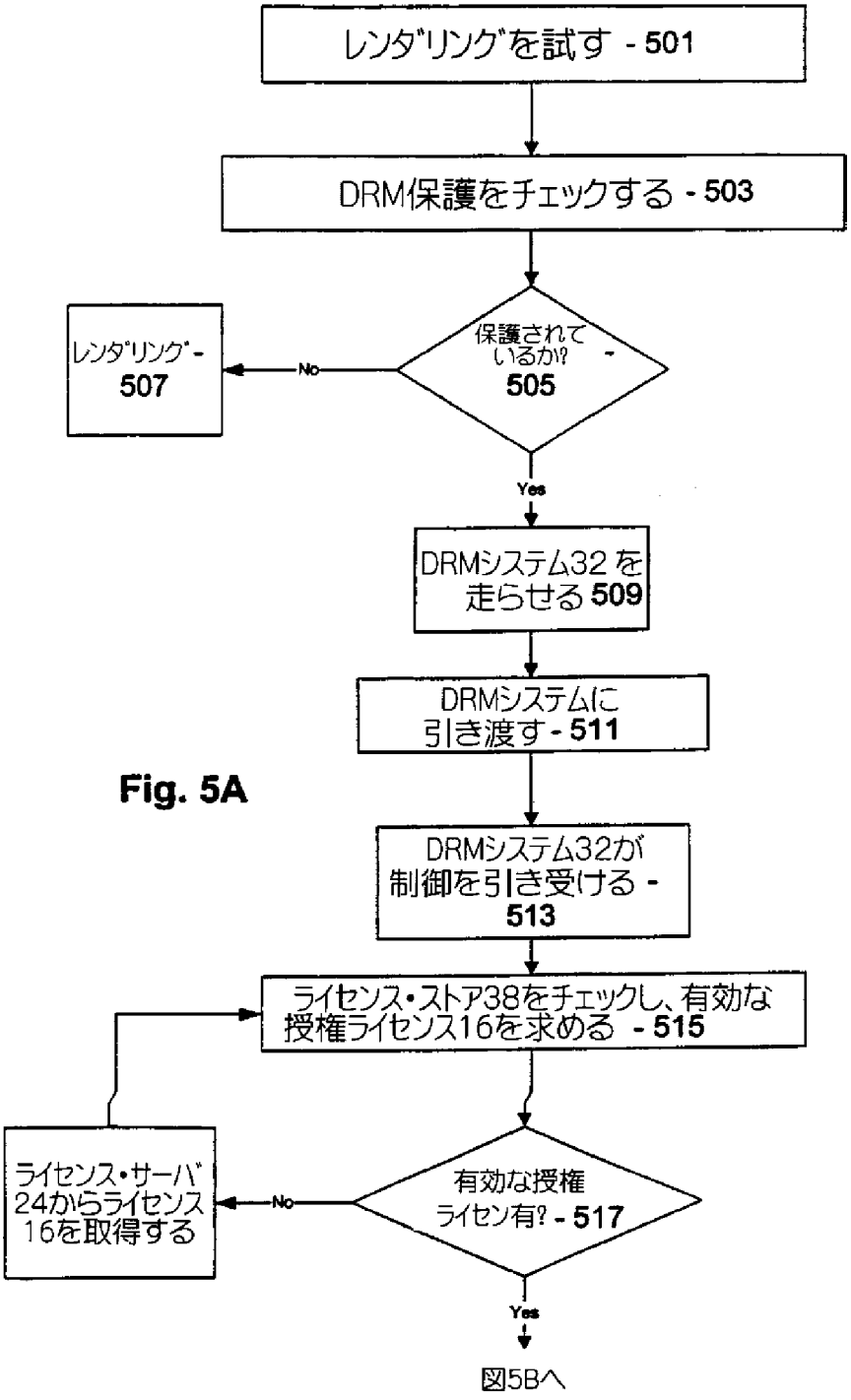

レンダリングを試す - 501
DRM保護をチェックする - 503
保護されているか? - 505
No
レンダリング - 507
Yes
DRMシステム32を走らせる 509
DRMシステムに引き渡す - 511
DRMシステム32が制御を引き受ける - 513
ライセンス・ストア38をチェックし、有効な授権ライセンス16を求める - 515
有効な授権ライセン有? - 517
No
ライセンス・サーバ24からライセンス16を取得する
Yes
図5Bへ

Fig. 5A

【図５Ｂ】

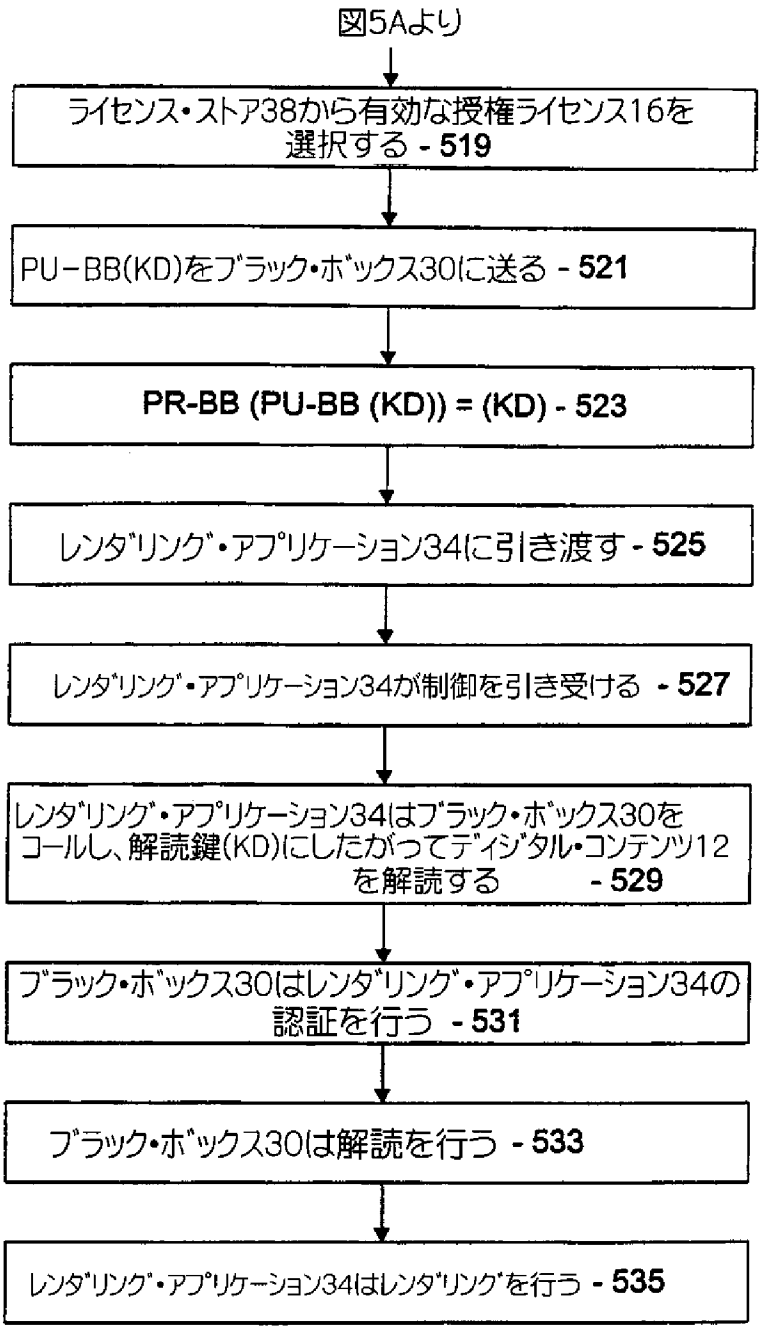
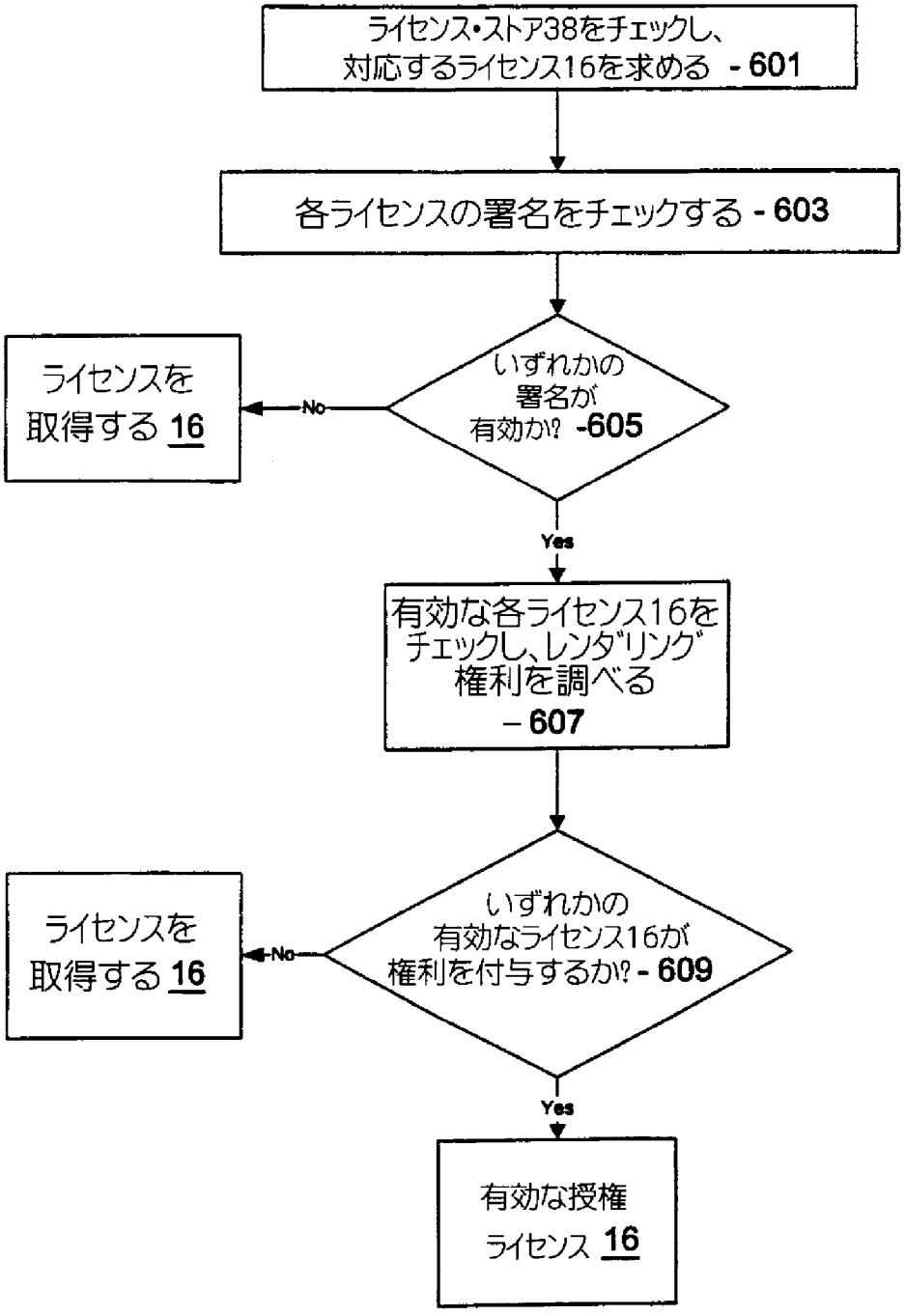


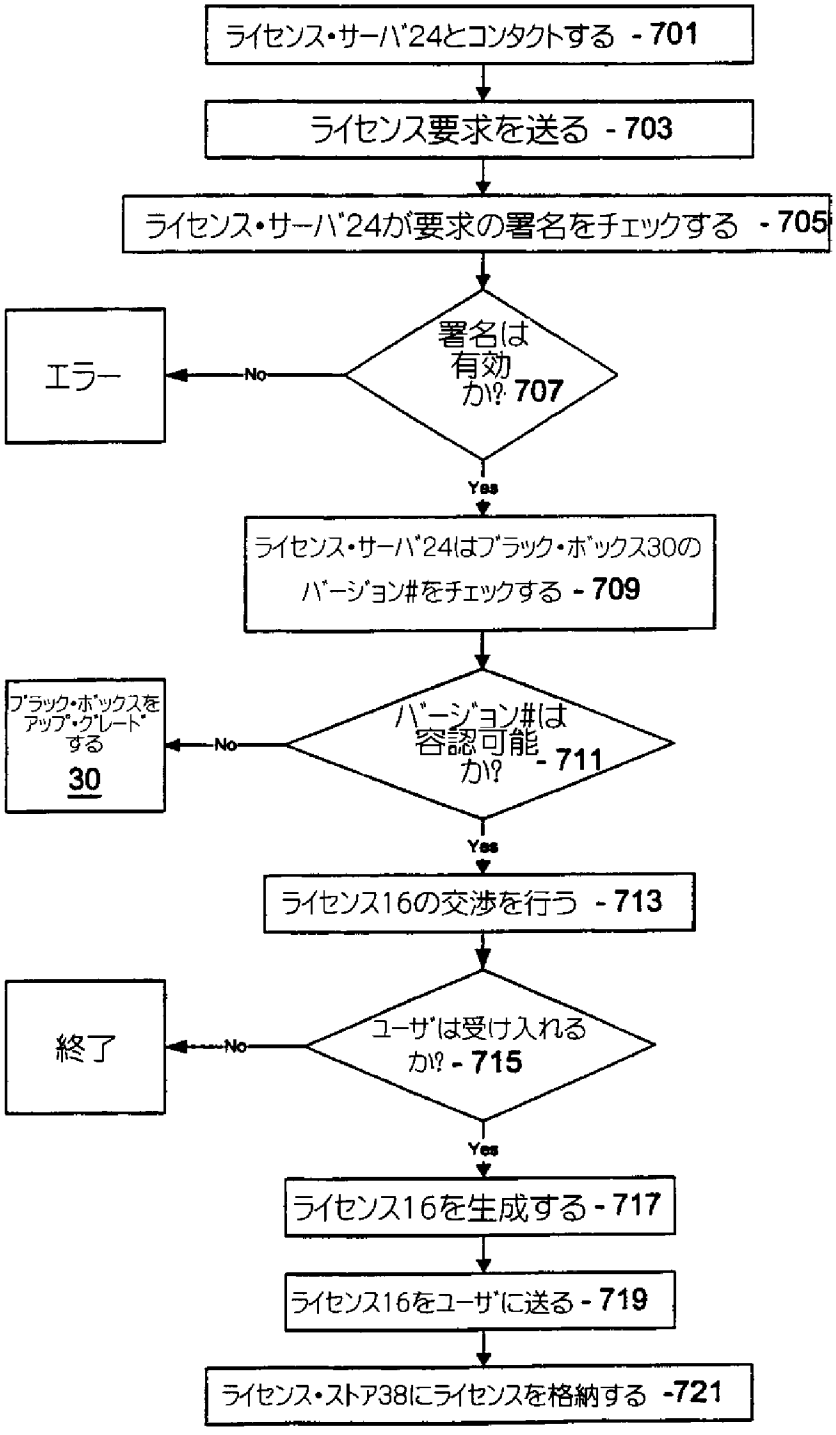
図5Aより
ライセンス・ストア38から有効な授権ライセンス16を選択する - 519
PU－BB(KD)をブラック・ボックス30に送る - 521
PR-BB (PU-BB (KD)) = (KD) - 523
レンダリング・アプリケーション34に引き渡す - 525
レンダリング・アプリケーション34が制御を引き受ける - 527
レンダリング・アプリケーション34はブラック・ボックス30をコールし、解読鍵(KD)にしたがってディジタル・コンテンツ12を解読する - 529
ブラック・ボックス30はレンダリング・アプリケーション34の認証を行う - 531
ブラック・ボックス30は解読を行う - 533
レンダリング・アプリケーション34はレンダリングを行う - 535

Fig. 5B

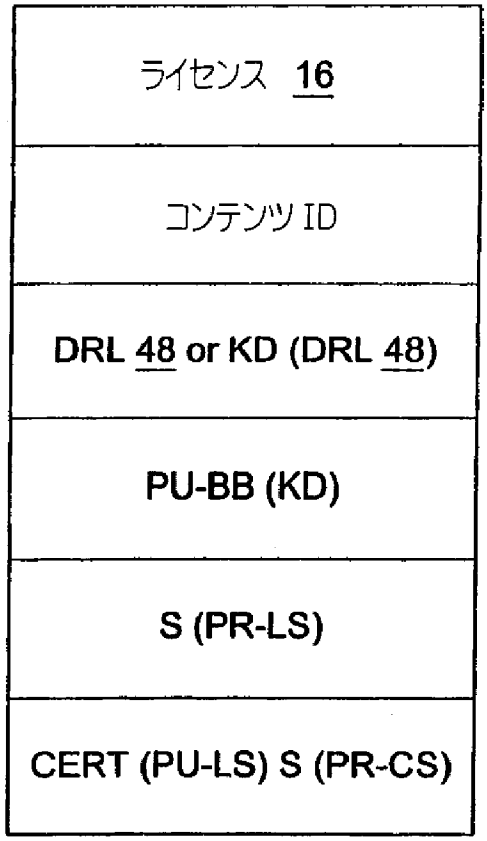
【図６】


ライセンス・ストア38をチェックし、
対応するライセンス16を求める - 601
各ライセンスの署名をチェックする - 603
いずれかの
署名が
有効か? -605
No
ライセンスを
取得する 16
Yes
有効な各ライセンス16を
チェックし、レンダリング
権利を調べる
– 607
いずれかの
有効なライセンス16が
権利を付与するか? - 609
No
ライセンスを
取得する 16
Yes
有効な授権
ライセンス 16

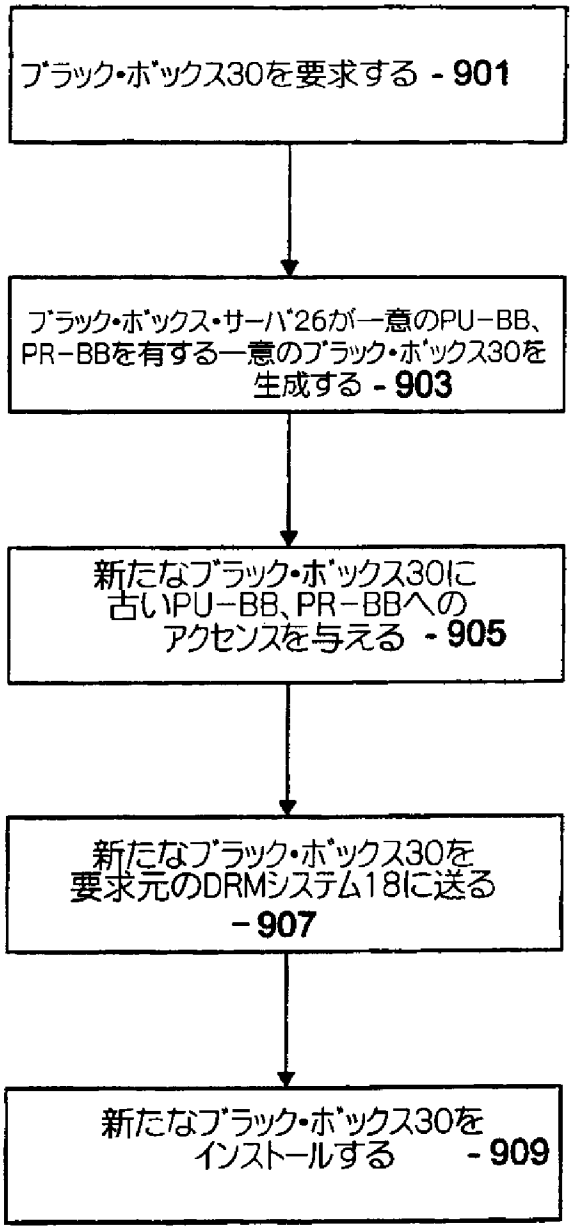
【図７】


ライセンス・サーバ24とコンタクトする - 701
ライセンス要求を送る - 703
ライセンス・サーバ24が要求の署名をチェックする - 705
署名は有効か? 707
No
エラー
Yes
ライセンス・サーバ24はブラック・ボックス30のバージョン#をチェックする - 709
バージョン#は容認可能か? - 711
No
ブラック・ボックスをアップ・グレードする 30
Yes
ライセンス16の交渉を行う - 713
ユーザは受け入れるか? - 715
No
終了
Yes
ライセンス16を生成する - 717
ライセンス16をユーザに送る - 719
ライセンス・ストア38にライセンスを格納する -721

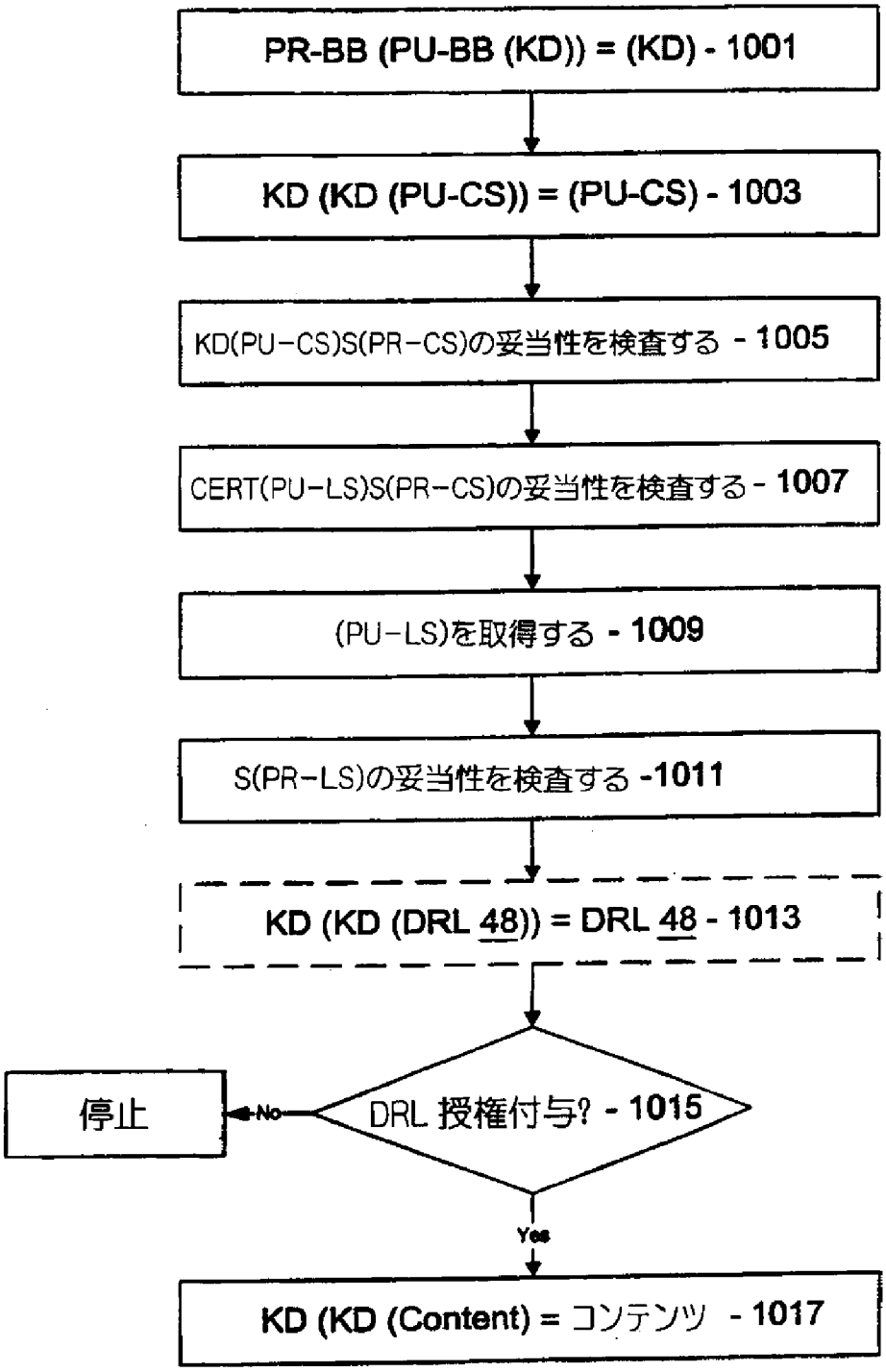
【図８】


ライセンス 16
コンテンツ ID
DRL 48 or KD (DRL 48)
PU-BB (KD)
S (PR-LS)
CERT (PU-LS) S (PR-CS)

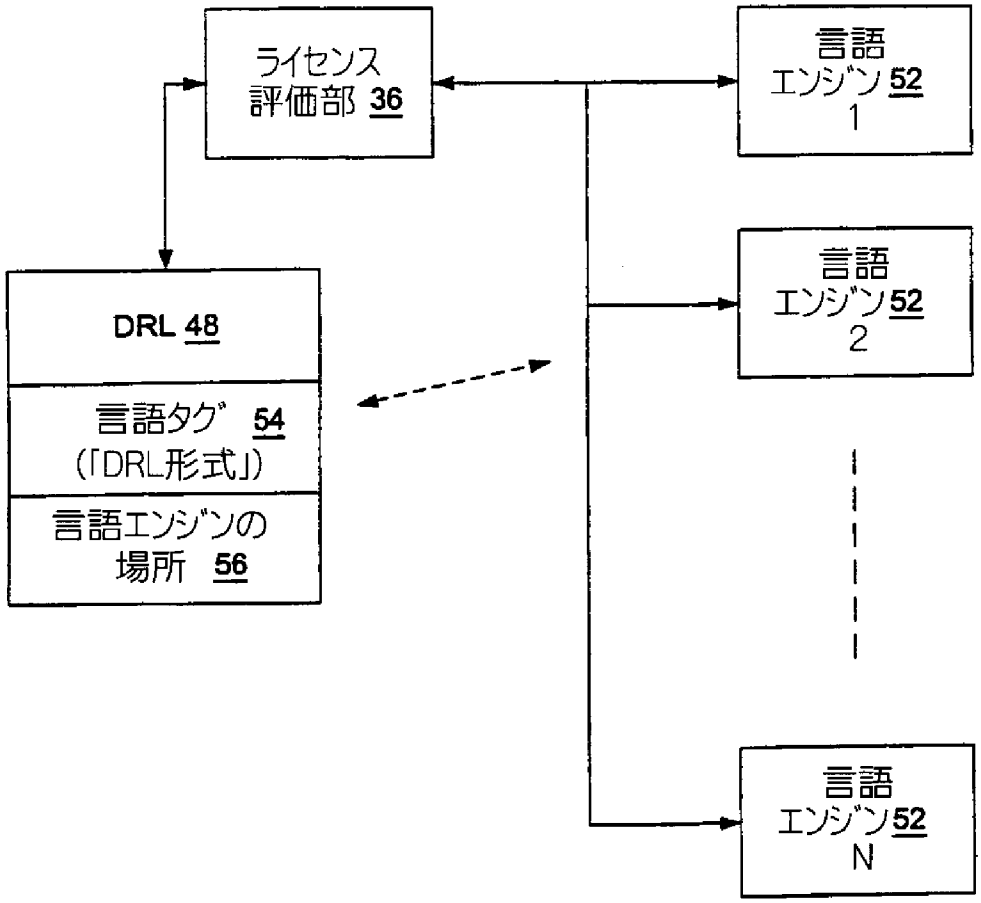
【図９】


ブラック・ボックス30を要求する - 901
ブラック・ボックス・サーバ26が一意のPU－BB、PR－BBを有する一意のブラック・ボックス30を生成する - 903
新たなブラック・ボックス30に古いPU－BB、PR－BBへのアクセスを与える - 905
新たなブラック・ボックス30を要求元のDRMシステム18に送る - 907
新たなブラック・ボックス30をインストールする - 909

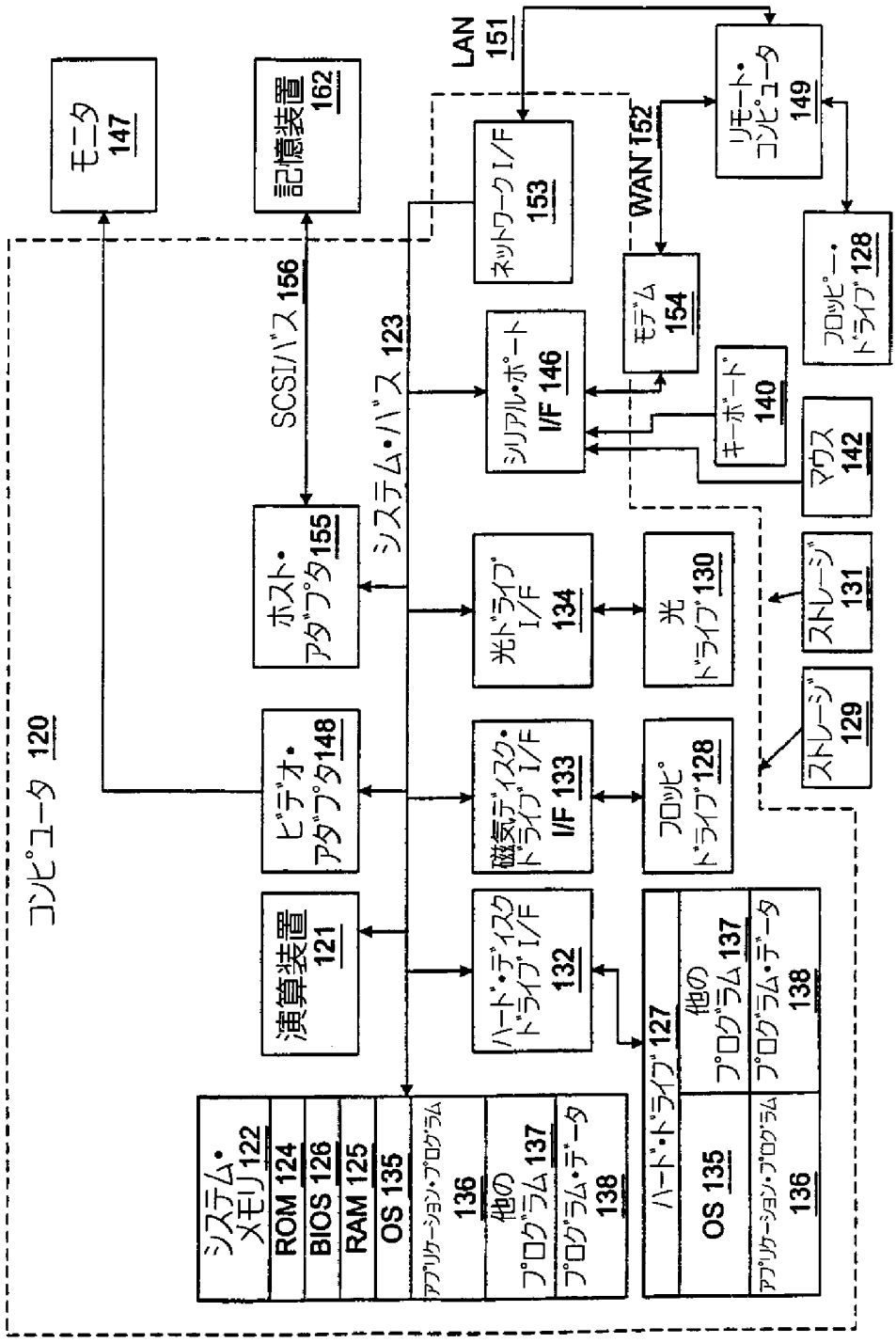
【図１０】


PR-BB (PU-BB (KD)) = (KD) - 1001
KD (KD (PU-CS)) = (PU-CS) - 1003
KD(PU-CS)S(PR-CS)の妥当性を検査する - 1005
CERT(PU-LS)S(PR-CS)の妥当性を検査する - 1007
(PU-LS)を取得する - 1009
S(PR-LS)の妥当性を検査する -1011
KD (KD (DRL 48)) = DRL 48 - 1013
DRL 授権付与? - 1015
No
停止
Yes
KD (KD (Content) = コンテンツ - 1017

【図１１】


ライセンス
評価部 36
言語
エンジン 52
1
言語
エンジン 52
2
DRL 48
言語タグ 54
(「DRL形式」)
言語エンジンの
場所 56
言語
エンジン 52
N

【図１２】


コンピュータ 120
モニタ 147
記憶装置 162
LAN 151
WAN 152
リモート・コンピュータ 149
SCSIバス 156
システム・バス 123
ネットワークI/F 153
モデム 154
プロッピー・ドライブ 128
シリアル・ポート I/F 146
キーボード 140
マウス 142
ホスト・アダプタ155
ビデオ・アダプタ148
光ドライブ I/F 134
光ドライブ 130
ストレージ 131
磁気ディスク・ドライブ I/F 133
プロッピー・ドライブ 128
ストレージ 129
演算装置 121
ハード・ディスク・ドライブ I/F 132
システム・メモリ122
ROM 124
BIOS 126
RAM 125
OS 135
アプリケーション・プログラム 136
他のプログラム 137
プログラム・データ 138
ハード・ドライブ 127
OS 135
他のプログラム 137
アプリケーション・プログラム 136
プログラム・データ 138

フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
		Ｈ０４Ｌ　9/00	６０１Ｅ

(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＬ，ＳＺ，ＴＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＲ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＤＭ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＡ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＴＺ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ

(72)発明者　アブブリ，ラジャセクハー
アメリカ合衆国ワシントン州98039，メディナ，ノースイースト・テンス・ストリート　7844
(72)発明者　ブリン，アーノルド・エヌ
アメリカ合衆国ワシントン州98004，ベルビュー，ノースイースト・トゥエンティセヴンス・ストリート　9401
(72)発明者　ジョーンズ，トーマス・シー
アメリカ合衆国ワシントン州98053－3618，レッドモンド，ノースイースト・シックス・ストリート　23617
(72)発明者　マンファーデリ，ジョン・エル
アメリカ合衆国ワシントン州98053，レッドモンド，トゥハンドレッドアンドフォーティフィフス・ウェイ・ノースイースト　7921
(72)発明者　ベル，ジェフリー・アール・シー
アメリカ合衆国ワシントン州98013，シアトル，ノース・シックスティセヴンス・ストリート　107
(72)発明者　ヴェンカテサン，ラマランスナム
アメリカ合衆国ワシントン州98052，レッドモンド，ノースイースト・トゥエンティセカンド・コート　17208
(72)発明者　イングランド，ポール
アメリカ合衆国ワシントン州98008，ベルビュー，ノースアップ・ウェイ　16659

(72)発明者　ジャクボウスキ，マリウス・エイチ
アメリカ合衆国ワシントン州98007，ベルビュー，ノースイースト・シックスティーン・プレイス　15212，ナンバー　28
(72)発明者　ユ，ハイ・イン・ヴィンセント
アメリカ合衆国ワシントン州98007，ベルビュー，ワンハンドレッドフォーティフォース・アベニュー・ノースイースト　809，ナンバー　シー－４

Ｆターム(参考)　5B085 AA08 BG04 BG07
5J104 AA16 EA04 EA15 MA01 MA05
NA02 PA07